

公 告 本		第94100710號實用新型 中文說明書修改正頁	
申請日 94年1月4日		公 告 日 94年4月16日	
案 番 50100170		A4 C4	
類 別 (以上各項有其異同)		514843	
發 明 新 型 專 利 說 明 書			
一、發明人 姓名 姓氏	中 文	實質萬得裝置及兼用處理方法	
	英 文		
二、創作人 姓名 姓氏	姓 名	田 道 駿 之 石 岩 駿 人 白 井 大 丈	
	國 際	① 日 本 ② 日 本 ③ 日 本 ④ 日 本 國 埼玉都川口市北品川六一七一三五 新規設計有限公司 ⑤ 日 本 國 埼玉都川口市北品川六一七一三五 新規設計有限公司	
三、受權人 姓名 姓氏	姓 名 (本稱)	新規設計有限公司 ヨシタ株式会社	
	國 際	① 日 本 ② 日 本 國 埼玉都川口市北品川六丁目七番三五號	
代 表 人 姓 名			
新規興成			

申請日期		92年1月4日		A4 C4
案號		90100370		
〔以上各欄全部用正楷寫〕				
發明專利說明書				
一、發明人 姓名 別號	中文			
	英文			
二、發明人 地址	姓 王		49 秋下裡	
	國 籍		地 日本	
註：日本圓鏡有限公司品司六一七一三五 號碼發給有限公司				
三、代理人 姓名 別號	姓 李		國 籍	
	(李國輝)		(李國輝)	
四、代理人 地址	姓 王		國 籍	
	(王國輝)		(王國輝)	
五、代理人 代表人 姓名 別號	姓 王		國 籍	
	(王國輝)		(王國輝)	

四、中大醫學檔案（醫學之名稱）

部。又，將存儲信息資料做為壓縮資料及極長處理程式，或壓縮程式種類的組合，使再生裝置，形成可判定可適用於壓縮存儲信息的再生處理程式。

#### 第六章 情境分类（按明之名制）

本机原厂皮带选用帝人碳纤维带（CFB）A450型（210×291公厘）

## 五、聲明說明( 2 )

惟而言，係將存儲信息資料之構成做為組合歷經資料及延長處理程式之構成，或將適用延長處理程式做為集管資訊並根據進行容納之歷旅資料存儲信息的集管資訊用以檢索抽出可適用之延長處理程式做為可用以執行再生選道。

本發明，某人製成 DVD、CD 等之記憶單體，或 CDTV、音頻網路，而且該單體以有形、無形各種訊號裝置之網絡而可得名之單音、重複、逆向、異式等之各種存儲信息，在使用者之所有的記憶過程中進行產生，並寄納於該記憶裝置，譬如記憶體卡、鍵盤、CD-R 等。同時利用前述於記憶單體之存儲信息時，用單項實現所有存儲信息並识别之希望的利用而得稱，兩項則被分配之存儲費用。在前述利用之外之第三者不被蓄意利用以達成某人所希望之目的。

七言詩集卷三

首先，若被程式，算符數量、圖像數量、文書作成次序等，使各項軟體資料（以下，稱此等為存儲信息（Content）），透過網絡網路之網路，或透過 D Y D 、  
CD 等可流逝的記憶體進行流通，此等之選存儲信息，係依用者所有之 Personal Computer ），關於上述軟體等之記錄再生概念的紀錄其量，譬如可容納的記憶卡、  
記憶碟等，一旦啟用後，係由容納該種傳輸再生形態可  
知。

譬如技術之影響遊戲選擇：PC 頂之資訊軟體由被接

五、睡眠障碍(一)

#### 【發明所屬之技術領域】

本章明，係有資料處理及統計五資料處理方法。更細而言，係有統以傳或質料存儲之資訊的正當性。即用以驗證有無察改之方法。較量，試子驗真之方法。又，有鑑在統處理所必要的別種驗題，如依據對應於各自別種驗題的主論兩面由進行而成。此可視得安全之鑑定方法。又，本章明，係提供用以辨析資料存儲信息之不同構成。具體而言，即用以認識並不尚稱據體而形成可用以排除存儲信息之不必要用的裝置及方法。達此本章明，係有號碼函可利用資料處理裝置之存儲信息。其他資料處理裝置中也可利用之存儲信息根據資料處理裝置固有之資訊等做為可容許進行鑑定之裝置及方法。惟在，若藉用以辨析資料存儲信息之資訊的正當性，即用以

进而，本发明，仅有关系式生成装置，存储信息资料生成方法，及资料整理方法，将共享资源，抽象资料，程式资料至另一种其为资料加以特征化处理，并将程式资料集一起储存于有组织的资料中，使存取信息利用者对再生、执行、或经修改装置进行重新处理等之操作，皆能提高存储信息资料有效管理之基础下而以实现形成可操作和利用之目的。

進而，係有關資料處理裝置、資料處理方法及存儲信息資料生成方法。用以提供有效執行被認證資料存儲信息之聲音資料、或有圖像資料等情形之再生處理的構成，用

Digitized by srujanika@gmail.com

### 五、骨膜說明(3)

用記憶卡裝置的主要構成要素，係具有：控制裝置，為動作控制；連接器，被選擇於控制裝置並為了連接於被裝在實質機械本體的切口；及非易失性記憶體等。被選擇於控制裝置並為了用以記錄資料。昇序於記憶卡之非易失性記憶體係藉由EEPROM，即電子記憶高密度構成。

被記錄於如此之記憶卡的資料，或程式等之名稱的存儲信息，係做為再生機器被利用由遊戲機器。P.C 等之資訊機器不應藉由使用者指示，或通過被連接之輸入装置由使用者之指示由非易失性記憶體被調用，並通過存取機器。

遊戲程式，音樂軟體，圖像軟體等，多數之軟體，下  
載後依舊，一般而言僅在其作者或，版權者擁有版權。  
因此，在此等之存儲信息的記存時，係固定之限制利  
用，即僅對正規之使用者，許可軟體之使用，並使未經可  
能的非正規，即非正規之使用者，無法存取。

對使用者以實質限制和用之 1 種方法，供配布存  
信息之暗號化處理。即，譬如通過網際網路等用以配布  
暗號化之聲音資料、圖像資料、遊戲程式等之各種存儲  
信息，同時僅對被認可並使用者的人，用以該項被配布  
暗號化存儲信息之裝置，即賦予該種結構之構成。

暗號化資料，係根據預定之手標碼由經密碼處理可得到利用之譯碼資料。在此如之資訊的暗號化處理使用暗號化鑰匙，在重號化處理使用譯碼化鑰匙之資料暗號化譯碼化方法係由前印即為某所周知。

A7  
B7五、發明說明（<sup>4</sup>）

在使用的時時化縮尾及津而化縮尾之資料增強化，詳述方法之懸掛者有各種的類型，故茲為其一例有別為所添共同論述增強化方式之方式。

共同論述增強化方式，係將使用於資料之增強化縮尾的增強化縮尾及使用於資料之津而化縮尾為共同論述，在正規之使用者賦予使用此等增強化處理，詳述之共同論述，由於未持有變之不正確使用者用以排除資料存取，在該方式之代變性的方式有 D E S ( 密料暗號標準 : Data Encryption Standard ) 。

被使用於上記之增強化處理，津而化縮尾的增強化縮尾，津而化縮尾，係譬如根據某進行字通用亂序碼 ( hash ) 函數等之方向性函數可取現。所謂之方向性函數，係指由其輸出字相對輸入底形非常因應之函數，譬如使用者決定要將字數為輸入一方而函數，譬如其輸出用以生成增強化縮尾，津而化縮尾，以期由此所取得之增強化縮尾，津而化縮尾，相反求出其原本之資料的進行字底實質上不可能。

又，在進行增強化時若由使用之增強化縮尾之處理，及在進行增強化時使用之津而化縮尾的增強化縮尾為不同算法之方式為易用所開闢論述增強化方式之方式，公開論述增強化方式，係由不特定之使用者使用可使用公開論述的方法，對於個人將津而化縮尾，難由公開論述被增強化之文書，係對於應用於其增強化處理之公開論述僅僅由秘

A7  
B7五、發明說明（<sup>5</sup>）

再生裝置 1 0 . 係為了用以執行資料存儲信息保在處理具有保序處理部 1 3 . 保存處理部 1 3 . 係用了用以防止被記憶於記憶裝置 2 0 資料的不正確使用，在資料用以實施增強化處理並用以執行保在處理。

再存儲信息是進行增強化時，係使用存儲信息暗號用輸出，存儲處理部 1 3 . 係用了用以存儲信息暗號用輸出，將存儲信息進行增強化，並持先後於 F P D ( 數顯 ) ，記憶卡，硬碟等之記憶裝置 2 0 之記憶部 2 1 。

使用者，係由記憶裝置 2 0 所以看出器存儲信息並進行再生，係由記憶裝置 2 0 所以看出器存儲信息並進行再生，並由記憶裝置 2 0 之記憶部 2 1 。

使用者，係由記憶裝置 2 0 所以看出器存儲信息並進行再生，並由記憶裝置 2 0 之記憶部 2 1 。

故依據圖 1 所示先將之標識，則以軟體，記憶卡等之記憶裝置 2 0 因為使用者存儲信息被帶號化，所以由另兩部或可防止不正確讀出，可是，將該軟體以其他 P C ，或記憶裝置等之資訊機器的再生裝置進行再生並加以利用，則同存儲信息無能，即爲了以津而化縮尾之存儲信息具有同津而化縮尾無所不同復則形不可再生。因此，將數之資訊機器中為了用以實現可利用之形態，將提供使用者之增強化縮尾有必要進行共因。

可是，將存儲信息之增強化縮尾進行共進化，並未持有所持之正規狀態之使用者將該過度之記憶無序狀態進行減退之可相性形成提高，由於未持有正規狀態之使用者形不成不能

A7  
B7五、發明說明（<sup>5</sup>）

密鑰形成可津而化縮尾，秘密論述，係僅使發行公開論述之個人所有，所以首由其公開論述被津而化縮尾者僅保持有密鑰形成個人可進行津而化縮尾，公其論述增強化方式之代性方式係有 R S A ( Rivest-Shamir-Adleman ) 暗號。

藉由利用如此的增強化方式，津而化縮尾存儲信息僅對正確使用者形可致而可津而化縮尾之系統，對於採用此等之增強化方式之智如技術的存儲信息配布構成後用圖 1 顯示加以說明。

圖 1 係顯示 P C ( 個人電腦 ) 、遊戲機器等之再生裝置 1 0 中，由 D V D 、 C D 3 0 、硬盤搭接 4 0 等之資料提供應用而再生獲得之程式，聲音資料，影像資料等 ( 存儲信息 ( Content ) )，同時由 D V D 、 C D 3 0 、網際網路 4 0 等所持取之資料被當可記憶於軟體，記憶卡，硬碟等之記憶裝置 2 0 的構成例。

程式，聲音資料，影像資料等之存儲信息，係採形成電氣化處理，並被提供於具有再生裝置 1 0 之使用者，正確使用者，採用以取得增強化處理，同時其增強化，將密鑰化縮尾之處於資料。

再生裝置 1 0 係具有 C P U 1 2 ，將輸入資料之再生處理在再生處理部 1 4 進行執行，再生處理部 1 4 . 係用以執行帶號化資料之津而化縮尾，進行提供之程式之再生，聲音資料，影像資料等存儲信息再生。

正確使用者，係得被提供之程式，為了再度使用在記憶裝置 2 0 進行深次 / 深次等，存儲信息之保存過程。在

A7  
B7五、發明說明（<sup>7</sup>）

防止存儲信息之不正確使用的缺點，以米持用正規狀態 P C ，過載後器等將消除不正確使用形態圖。

又，將存儲信息及記憶卡等，據據機進行共用化，係由一台之機器使其存儲資訊與一接觸時，便波及被接觸範圍會形成使用該機器之系統全體。

進而，如上述將各部進行共同化之環境中，係譬如在某 P C 上被使用，因被保存於記憶卡，軟盤等之記憶裝置的增強化之存儲信息，係在另外之狀象可容易複雜，並非原本之存儲信息資料形底可使用被接觸點之利用形態，在連載機器，P C 等資訊機器中便可利用之存儲信息資料被多數接觸，或機會行被篡改之可能性。

## 【發明所欲解決之問題】

存儲信息資料之之實質，即爲了用以狀存被接觸點之核對證用之核對證於存儲信息資料，記錄再生過程中，根據驗証對象之資料全體結合於生成之核對值及存儲信息資料的核對被藉由核對處理，使進行資料驗証之方法由先前被進行。

可是，對資料存儲信息之核對值，係對資料全體被生成為一致性，對資料全體被用以執行被生成之核對值的核對處理，對成為核對對象之資料全體形必需要用以執行核對值生成處理，譬如 D E S - C B C 模式中難由生成之信息認證符號 ( M A C ) ，進行求出核對值 I C V 方法時，對資料全體形必需要用以執行 D E S - C B C 標準。詳計



A7  
B7五、發明說明（<sup>13</sup>）

端號或標記，對應追存錄信函資料用以執行編號處理，及

控制部，對前述追號處理部用以執行控制；

而前述追號處理部，其構成係具有：

消存錄信函資料構成部分函件匯集部之部分資料對合上以上部分資料與各函件為核對值並用以生成部分函件對值，經由該函件生成之部分函件對值則對應用以執行前述消存錄信函資料之新函萬能；同時

至少再將前述部分函件對值匯集合上以上部分函件對值集合用以形成中間核對值，並使該生成之中間核對值，對應於用以構成前述部分函件對值集合之匯數的部分函件對值及前述部分函件對值集合全體用以執行辨証成績。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分函件對值，係將形成核對值之部分資料作為信息，藉由用以選用部分函件對值生成結果之略號處理被生成之值，而前述中間核對值，則將前述之部分函件對值及前述資料列數為信息，藉由選用部分函件對值生成結果之略號或短號生成之值，而前述消存錄或新函，其構成係具有用以審核前述部分函件對值生成結果及前述函件對值生成結果。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述追號處理部，係具有複數級層之部分函件對值生成結果，及用以執行資料驗證訊號之各個的置換固有之装置還有各名稱號。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述消存錄或新函。

本執業人送達中國國家商標局(CNNSM44)申請(200\*207公釐)。 - 15 -

A7  
B7五、發明說明（<sup>14</sup>）

據為：前述資料處理裝置，係做為前述複數之各名稱號，凡具有用以執行資料驗證訊號共同於系統之全體性的共同署名稱號，及用以執行資料驗證訊號之各個的置換固有之装置還有各名稱號。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分函件對值，所含之各部分函件對值，對於用以構成資料之一部分的幾當部內資料生成1以上；及反向該信息對值，對於用以構成資料之一部分的存儲信息對值，對於用以構成資料之一部分的存儲信息對值全部用以生成函件對值並藉由用以執行核對處理，進而，根據前述消存錄或新函內部內資料之部分資料對值並用以執行核對處理，進而，根據前述消存錄或新函內部內資料之部分資料對值並用以生成函件對值全部用以生成函件對值並藉由用以執行核對處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分函件對值，函件對值部分函件對值，對於用以構成資料之一部分的幾當部內資料生成1以上，前述消存錄或新函部，其構成係具有對於前述幾當部內資料之部分資料集合用以生成1以上之各部分函件對值並用以執行核對處理；鑑而，用以構成消存生成之值1以上的各部分函件對值及前述資料之一部分函件對值全部用以生成函件對值並藉由用以執行核對處理用以執行資料驗證。

本執業人送達中國國家商標局(CNNSM44)申請(200\*207公釐)。 - 17 -

A7  
B7五、發明說明（<sup>15</sup>）

據為：前述追號處理係DES單字處理，而前述略號處理係，係具有可執行DES單字處理之構成者。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分函件對值，係將形成核對對象之部分資料作為信息在DES-CBC模式中被生成之信息認證符號(MAC)，而前述中間核對值，係將形成核對對象之部分資料對值集合資料列數為信息在DES-CBC模式中被生成之信息認證符號(MAC)，而前述追號處理部，係具有由前述DES-CBC模式用以執行非對值處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：藉由具有前述追號處理部之DES-CBC模式的兩處處理構成，係僅在形成處理對象之信息對的一部份被適用三倍的DES之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係具有署名論述，而前述追號處理部，係對前述中間核對值由適用前述署名論述將被生成之值為了資料驗證係將核對值並進行適用之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係將具有署名論述將被形成之署名論述，而前述追號處理部，係具有標識的核存並借由資訊之限制利用選擇由署名之署名論述將被選擇之署名論述將被形成之署名論述將被選擇之署名論述對前述中間核對值進行適用的研發過程為了資料驗證係將核對值之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特

本執業人送達中國國家商標局(CNNSM44)申請(200\*207公釐)。 - 16 -

A7  
B7五、發明說明（<sup>16</sup>）

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係與前述特徵為：在前述追號處理部中具有紀錄装置用以執行正當性驗證之接執行的資料。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置之中部分函件對值的核對處理中，在狀態成立核對時，其特徵為：前述追號處理部，係對前述記錄裝置具有用以中止容納處理之構成者。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，述其特徵為：在前述略號處理中具有再生處理部用以執行資料驗證之核對執行資料者。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述略號處理部中之部分函件對值的核對處理中，在狀態成立前成立時，其特徵為：前述追號處理部，係在狀態再生處理部具有用以中止再生處理之構成者。

進而，本發明之第2側面，

係一張資料處理裝置，藉由記憶媒體隨身通訊裝置進行提供之前述資料的處理，其特徵在於具有：

增號處理部，對於存儲個信息資料用以執行核對處理

本執業人送達中國國家商標局(CNNSM44)申請(200\*207公釐)。 - 18 -

五、發明說明（<sup>15</sup>）

引剖部，對前述每個處理過程用以執行控制；

而前述每個處理部，其構成係具有：

前述對象資料係依循號化資料項，藉由該號化資料之譯碼處理對被取得資料項用以執行該計算處理對被取得到算得資料項用以用實作通用名稱點之暗號處理，用以生成該驗證對象資料項之暗號對值。

進而，本發明之資料處理方法之一實施態樣中，前述演算處理，其特徵為：藉由前述暗號化資料之譯碼處理對被取得資料項用以預定組元單位進行操作性演算和演算之處理。

進而，本發明之第3剖面。

係一種資料處理方法，而由前述選擇資訊選擇並進行被提供之存儲信息資料的處理，其特徵在於：

將前述資料項構成部分組成數個部分之部分資料集合1以上部分資料集合為候對該並用以生成部分核算對值，藉由用以候對該並用以生成部分核算對值之暗號用以執行前述部分資料之驗證處理。

至少將前述部分核算對值根據集合1以上部分核算對值集合用以生成中間核算對值，並使用該生成中間核算對值用於以構成前述部分核算對值集合之數個部分核算對值並動之部分資料集合全體用以執行該驗證處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述部分核算對值，係將形成為對象之部分資料做為相應，具有藉由用以應用部分核算對值生成點號之暗號。

本辦法是適用中國國家標準(CNS/IAI規範(210+207公量)) - 19 -

(資料處理方法之各個處理部之各個處理點之暗號點號)

(資料處理方法之各個處理部之各個處理點之暗號點號)

五、發明說明（<sup>15</sup>）

處理之各個核算部有的裝置固有著名點號依據資料之限制利用舉標並加以應用。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：

前述部分核算對值，係由：某幾部分核算對值，對於用以構成資料之部分的業務內部用以生成1以上；及存儲信息點號對值，對於用以構成資料之部分的存儲信息內部用以生成1以上；前述資料點號對值，係對於前述業務內部資料之部分資料集合用以生成1以上之某幾部分核算對值用以執行核對處理，進而，前述資料生成之前述業務部分核算對值及前述資料點號對值全部用以生成該核算對值並用以執行資料點號對值。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：

前述部分核算對值，係含某部分核算對值，對於用以構成資料之部分的業務內部資料用以生成1以上，前述資料點號對值，係對於前述業務內部資料之部分資料集合用以生成1以上之某幾部分核算對值並用以執行核對處理，進而，用以構成資料之部分核算對值並用以執行該計算處理，前述資料之部分核算對值用以存儲信息並向步驟所構成資料點列用以生成該點對值並藉由用以執行核對處理用以執行資料點號對值。

本辦法是適用中國國家標準(CNS/IAI規範(210+207公量)) - 21 -

五、發明說明（<sup>15</sup>）

進而，本發明之資料處理方法之一實施態樣中，其特徵為：資料之驗證狀，進而將驗證完成資料點號進行寄送於記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，前述部分核算對值之候對處理中，便核對未能成立之情形中，其特徵為：用以中止者納處理到前述記錄装置並用以執行控制。

進而，本發明之資料處理方法之一實施態樣中，前述部分核算對值之候對處理中，其特徵為：複用以執行資料之單質部分核算對值的核對處理，將成立某單質部分核算對值的資料傳送到前述再生處理部並可再生並用以執行控制。

進而，本發明之第4剖面。

係一種資料處理方法藉由記憶裝置及訊息傳遞進行被提供之存儲信息資料之處理，其特徵在於：

前述對象資料係依循號化資料項，藉由該號化資料之譯碼而處理對被取得之譯碼資料用以執行該算處理。

藉由前述演算處理對被取得之譯碼資料用以生成該點號藉由用以執行通用名稱點號之暗號處理用以生成該驗證對象資料之核對。

本辦法是適用中國國家標準(CNS/IAI規範(210+207公量)) - 22 -





五、發明說明（<sup>25</sup>）

傳送資料之傳送到來或轉送至的外部連接裝置之認證處理，而前述裝置生成步驟，係指適用以生成此外部連接裝置之認證號碼 Kake 的認證號碼生成用主編號 Mcake，及前述外部連接裝置之認證號碼生成步驟的外部連接裝置號碼子用以執行確認處理，並用以生成前述外部連接裝置之認證號碼 Kake 的認證號碼生成步驟，而前述裝置認證處理步驟，係根據前述認證號碼生成步驟中進行生成之認證號碼 Kake 用以執行外部連接裝置之認證處理的步驟。

進而，本發明之資料處理方法之一實驗態樣中，其特徵為：

前述資料處理方法中之進行執行的資料處理，係對資料之名稱處理，而前述裝置生成步驟，係根據用以生成前述資料處理裝置之資料處理裝置名稱如 Kdev 的署名識別生成用主編號 Mcake，及前述資料處理裝置之資料處理資料的資料處理裝置別子用以執行確認處理，並用以生成前述資料處理裝置之資料處理裝置名稱如 Kdev 的署名識別生成步驟，而前述裝置處理步驟，係根據前述資料名稱生成步驟中進行生成之署名識別 Kdev 用以執行該資料之名稱處理的步驟。

進而，本發明之資料處理方法之一實驗態樣中，其特徵為：前述裝置生成步驟，係依據被處理對象之其後或資料之其後資料至少一部分做為信息，並所將述論點作為資訊識別進行適用之認證處理。

進而，本發明之資料處理方法之一實驗態樣中，其特

五、發明說明（<sup>33</sup>）

進而，本發明之第 1 例面。

係一種資料處理方法，藉由複數之資料處理裝置被構成資料處理系統中之資料處理方法，其特徵為：

在前述複數之資料處理裝置中之 1 個資料處理裝置 A 中，根據存儲信息識別生成用主編號為用以生成或適用於存儲信息資料之認證處理號碼子，及該資料處理裝置 A 之新舊識別子藉由前述存儲信息識別號碼子被轉換之存儲信息資料分析於記憶算盤之步驟，在不同資料處理裝置 B 中，根據前述資料處理裝置 A 及同一之前述存儲信息識別號碼子及前述資料處理裝置 A 之裝置識別號碼子用以生成前述存儲信息識別子及同一存儲信息識別號碼子，及在前述資料處理裝置 B 藉由生成之存儲信息識別子執行前述的記憶算盤之存儲信息資料之演算之步驟。

進而，本發明之第 1 例面。

係一種資料處理方法，由主與次，及形成該主與次之認證易近對象的裝置所構成之資料處理系統中之資料處理方法。

前述副裝置，係根據該認證號碼生成用主編號為用以生成或適用於主與次及副與次間之認證處理之認證號，及該副裝置之認證別子的副裝置識別號碼子用以生成認證號碼，並將生成之認證號碼子寄存於副裝置內之記憶體。

前述主裝置，係根據前述認證號碼生成用主編號，及前述副裝置之認證別子的副裝置識別號碼子用以生成認證號碼並用以執行認證處理。

五、發明說明（<sup>25</sup>）

微路，而前述號碼規係適用 D E S 算法之密碼處理。

進而，本發明之第 10 例面。

係一種資料處理方法，由提供存儲信息資料之存儲信息資料利用供應、及進行存儲信息資料之利用的存儲信息資料利用供應所構成資料處理系統中之資料處理方法，其特徵為：

前述存儲信息資料提供裝置，係根據據為用以生成適用於存儲信息資料之認證處理的存儲信息資料配對號碼子，及根據該配對號碼子配對號碼子用以存儲號碼及前述存儲信息資料別子而用以生成複數不同之存儲信息資料配對號碼子，藉由該存儲信息資料之配對號碼子用以執行認證處理並用以生成前述密鑰之密鑰化資料處理資料，而前述存儲信息資料利用供應，係具有前述各個信息資料提供裝置之認證號碼之四倍之配對號碼之三至 1 倍之配對號碼子生成用主編號，及同時配對號碼子生成用主編號子藉由被生成之配對號碼子區分化存儲信息資料進行認證。

進而，本發明之資料處理方法之一實驗態樣中，其特徵為：

前述存儲信息資料提供裝置，係具有複數不同之配對號碼子用以存儲號碼為用以生成複數不同之存儲信息資料配對號碼子，並根據該配對號碼子配對號碼子用以存儲號碼及前述存儲信息資料別子而用以生成複數不同之存儲信息資料配對號碼子，藉由該存儲信息資料之配對號碼子用以執行認證處理並用以生成前述密鑰之密鑰化資料處理資料，而前述存儲信息資料利用供應，係具有前述各個信息資料提供裝置之認證號碼之四倍之配對號碼之三至 1 倍之配對號碼子生成用主編號，及同時配對號碼子生成用主編號子藉由被生成之配對號碼子區分化存儲信息資料進行認證。

五、發明說明（<sup>33</sup>）

進而，本發明之第 13 例面。

係一種程式提供裝置，用以提供權限程式並用以執行資料轉換裝置，資料轉換裝置，認證處理，署名審查至少其中之一的類別處理並將認證號碼在電腦系統上執行之程式提供裝置，其特徵為：

前述認證程式，係含有：

將執行號或識別之識別號碼，根據主編號為用以生成或適用於前述號或識別號碼之認證號碼，及該號或識別對象之其後或資料之識別號碼子進行生成之識別號碼子步驟；及

藉由前述號或識別號碼子進行生成之識別號碼子用以執行前述號或識別號碼子步驟。

本發明之第 14 例面。

一種資料處理裝置，係藉由記憶媒體或通過訊號媒體進行提供存儲信息資料之處理的資料處理裝置，其特徵為於具有：

記憶部，用以容納資料處理裝置別子：

名單檢驗部，用以列出並合於存儲信息資料中之不正確號碼名單，並用以執行該名單中之參加者及被容納於前述記憶部之前述資料處理裝置別子之對應處理；及

控制部，指該裝置對處理裝置中之核對結果，並含有在前述不正確號碼名單中與前述資料處理裝置別子一致的資訊時，用以中止對前述資料處理裝置之再生或記錄其對應的審查至少其中之一的處理執行。

進而，本發明之資料處理裝置之一實驗態樣中，其特



五、發明說明（<sup>35</sup>）

唯使處理部，對前述存儲信息資料用以執行縮號處理。

控制部，對前述縮號處理部用以執行控制；

系統共同聯繫部，被使用於前述縮號處理部中之縮號處理，並共同於利用前述存儲信息資料之其他資料處理裝置；及

獎勵固有識別子至少其中之一，為了用以生成並被使用於前述縮號處理部中之縮號處理的資料處理裝置固有之装置固有縮號或該装置固有縮號；

而前述縮號處理部。

係根據前述各個信息資料之利用規則將前述系統共同聯繫，獎勵固有識別子之中之一適用於前述存儲信息資料並用以執行縮號處理。

述而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述縮號處理部，其構成具有根據獎勵於前述存儲信息資料之利用規則利用資訊而將前述系統共同聯繫，而前述獎勵固有識別子中之一適用於前述存儲信息資料並用以執行縮號處理。

進而，前述縮號處理裝置之一實施態樣中，其特徵為：前述獎勵固有縮號，係述而，具有記錄裝置用以記錄前述存儲信息資料。而前述縮號處理部，係根據前述存儲信息資料僅僅在自己之資料處理裝置並附有使用之限制利用時，對前述個別信息資料用前述裝置固有縮號用以執行縮號處理並用以生成可得名稱縮號。並將前述存

五、發明說明（<sup>37</sup>）

前述存儲信息資料放在自己之資料處理裝置以外也可做為使用時，對前述存儲信息資料使用前述系統共同聯繫用以執行縮號處理並用以生成前述資料用前述縮號。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係具有資料處理裝置固有之著名縮號 Kdev，及在複數之資料處理裝置共同之系統著名縮號 Ksys，而前述縮號處理部，係將前述存儲信息資料僅放在自己之資料處理裝置並附有使用之限制利用而寄納於前述記錄裝置，對前述存儲信息資料並用前述裝置固有縮號對錯，前述存儲信息資料放在自己之資料處理裝置以外的獎勵也後為可使用並寄納於前述記錄裝置，對前述存儲信息資料適用前述系統著名縮號 Ksys 種由轉換或處理用以生成縮號對錯，而前述縮號處理部，係將前述縮號處理部之獎勵的前述存儲信息資料固有縮號或前述縮號對錯其中之一與前述存儲信息資料一起寄納於前述記錄裝置並用以執行控制。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，其構成係具有資料處理裝置固有之著名縮號 Kdev，及在複數之資料處理裝置共同之系統著名縮號 Ksys，而前述縮號處理部，係僅在自己之資料處理裝置並附有使用之限制利用的存儲信息資料時，對前述存儲信息資料適用前述裝置固有之著名縮號 Ksys 種由縮號處理用以生成獎勵固有之著名縮號 Kdev，藉由縮號處理用以生成獎勵固有縮號對錯，並用以執行前述存儲信息資料固有縮號對錯的縮對處理，放在自己之資料

五、發明說明（<sup>38</sup>）

前述裝置以外的獎勵也被做為可使用用以再生並附有限制利用之存儲信息資料時，對前述存儲信息資料適用前述系統著名縮號 Ksys 有由單式處理用以生成縮號對錯，並用以執行該對錯並從之後之縮號對錯的限制獎勵，而前述縮號處理部，係獎勵固有縮號對錯成立之後之情形，或僅將前述縮號對錯對應於成立之後之情形以形成獎勵信息資料之縮號處理並使獎勵進行並用以生成可得名稱縮號。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，其構成係具有記錄資料處理裝置固有縮號 Kdev，及實質運算獎勵固有名稱縮號子 IDdev，而前述縮號處理部，係根據前述獎勵或獎賞裝置固有名稱子 IDdev 及前述資料處理裝置固有名稱縮號子 IDdev 種由縮號處理用以生成可得名稱縮號 Kcav。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述縮號處理部，其構成係分別對前述資料處理裝置固有名稱子 IDdev 應用前述獎賞或獎賞裝置固有名稱子 IDdev 並附有使用之限制利用時，對前述存儲信息資料並用前述獎賞或獎賞裝置固有名稱子 IDdev 並附有使用之限制利用而執行縮號處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述縮號處理部，其構成係將前述存儲信息資料分

五、發明說明（<sup>39</sup>）

將成複數部分後之部分資料對合 1 以上部分資料與合主導號處理用以生成部分板級對錯，合生成之後之部分板級對錯對錯部分對錯兼合資料判斷由縮號處理用以生成中間板對錯。

進而，本發明之第 1~9 號置。

係一種資料處理方法，藉由記錄裝置或通訊裝置進行被後存儲信息資料之處理的資料處理方法，其特徵在於：

根據前述存儲信息資料之利用規則。

以選擇選擇前述存儲信息資料共連於其他資料處理裝置之縮號處理或理用系統共同聯繫，或，資料處理供應固有之後置固有縮號對錯其中之一的縮號處理縮號。

將選擇之後之縮號處理縮號適用於前述存儲信息資料用以執行縮號處理。

進而，本發明之資料處理方法之一實施態樣中，對前述資料處理方法之中之存儲信息資料的記錄裝置之記錄處理中，其特徵為：前述存儲信息資料僅放在自己之資料處理裝置並附有使用之限制利用時，對前述存儲信息資料並用前述裝置固有縮號對錯用以執行縮號處理並用以生成可得名稱縮號對錯前記錄裝置，而將前述存儲信息資料也放在自己之資料處理裝置以外做為可使用時，對前述存儲信息資料用前述系統共同聯繫用以執行縮號處理並用以生成可得名稱縮號對錯前述記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，對前述

## 五、發明說明（45）

述資料處理方法中之存儲信息資料的記錄次僅之記錄處理中，其特徵為：將前述存儲信息資料備置在自己之資料處理裝置而後用於使用之限制利用並啟動前述記錄裝置時，對前述存儲信息資料適用前述存儲装置固有之名稱稱之 Kdev 之後再由存儲裝置用以生成對值，將前述存儲信息資料與自己之資料處理裝置以外的設備連為可使用並容許於前述記錄裝置時，對前述存儲信息資料適用前述系統固有之名稱稱之 Ksys。後藉由前述處理用以生成總核對值。

並非前述生成之後前述存儲裝置有核對值或前述總核對值其中之一與前述存儲信息資料一起存於前述記錄裝置。

而今，本發明之資料處理方法之一實施態樣中，對前述資料處理方法中之存儲信息資料的再生處理中，其特徵為：前述在自己之資料處理裝置用以再生被賦有使用之限制利用後的存儲信息資料時，對於前述存儲信息資料適用前述固有之名稱稱之 Kdev。後藉由前述處理用以生成總核對值，並足以執行前述生成之後固有核對值的核對處理，也故在自己之資料處理裝置之外之存儲裝置為可使用並有限制利用後用以再生存儲信息資料時，對前述存儲信息資料適用前述其固有之名稱稱之 Ksys。後藉由前述處理用以生成總核對值，並用以執行前述或之後之核對總對值的核對處理。成立前述新裝置有核對值之核對係用以執行前述存儲信息資料之再生。

本發明是適用於半導體裝置（CNS344A 機械（210×207 公厘） - 43-

## 五、發明說明（45）

述而，本發明之資料處理方法之一實施態樣中，其特徵為：由根據資料處理裝置著名而此用之名稱稱之 Mkdev 及資料處理裝置固有之名稱稱之 IDev 與由研磨及壓縮而有絲狀用以生成等名稱稱之 Kdev 之步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述著名稱為 Kdev 之步驟時，係對前述存儲信息資料用以執行前述處理用以生成中間核對值之步驟，在前述中間對該對值前述資料處理裝置固有絲狀或系統共用論底後用以進行相應處理。

而今，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係前述，將前述存儲信息資料分割成數個部分之後之部分資料對合在 1 以上部分資料集合而由總號處理用以生成部分核對值，對合該生成之後之部分板對值之部分核對值集合資料列由總號或單用以生成中間核對值。

而今，本發明之第 20 步驟。

係一種程式提供軟體，提供電腦程式藉由記憶體或讀寫頭進行該提供存儲信息資料之處理將資料處理在電腦系統上執行之程式標稱體，其特徵為：

## 五、發明說明（45）

根據前述存儲信息資料之利用狀態。

用以選擇利用前述存儲信息資料共通於前述資料處理裝置之固有之資料處理裝置用以再生前述存儲裝置固有之與前述固有之核對其之一的時脉處理裝置之步驟。

則選擇之後前述處理裝置用以執行前述存儲信息資料用以執行前述步驟。

而今，本發明之第 21 步驟。

係一種資料處理裝置，前述記錄裝置該述資訊元件道而該提供存儲信息資料之處理的資料處理裝置，其特徵在於其具有：

資料處理部，對前述存儲信息資料用以執行前述處理；及

限制部，對前述號號處理所用以執行限制；

前述這些處理部。

述在於前述資料驗證對象之存儲信息資料單位用以生成前述存儲信息核對值，藉用以執行前述之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息資料單位的正當性驗證處理。

而今，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，其構成具有存儲信息核對值生成處，前述號號處理部，保有驗證對象之存儲信息資料用以生成前述存儲信息核對值之後用以執行前述處理並用以生成前述存儲信息核對值。

本發明是適用於半導體裝置（CNS344A 機械（210×207 公厘） - 45-

## 五、發明說明（45）

述而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述編號處理部，係用以驗證對象之存儲信息區段資料被帶號號化時，藉前述存儲信息區段資料之擇號處理將依據前述譯文全體以指定給光單位進行指定之撰寫處理並用以生成存儲信息中間體，使驗證對象之存儲信息區段資料未被帶號號化時，藉存儲信息同步資料被帶號號化時應用前述指定之撰寫處理以生成存儲信息中間體。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：在前述編號處理部之前述中間核對值的生成處理進行前述前述之撰寫處理後之核對值和。

而今，本發明之資料處理裝置之一實施態樣中，其特徵為：前述增強號處理部，係藉由 C B C 模式具有帶號處理構成，並使增強號對象之存儲信息同步資料被帶號號化時應用於存儲信息中間核對值之前述之撰寫處理，係藉由 C B C 模式之撰寫處理。

而今，本發明之資料處理裝置之一實施態樣中，其特徵為：前述增強號處理部，係構成在存儲信息區段資料合有複數之帶號，並使前述各許存儲信息區段資料的一部分之零件有驗證對象時，藉據驗證對象零件用以生成存儲信息核對值，並藉由用以執行前述之存儲信息核對值的核對處

本發明是適用於半導體裝置（CNS344A 機械（210×207 公厘） - 46-

五、發明說明（<sup>44</sup>）

這，用以執行前述資料中之各存儲信息區段資料單位的正常性驗證處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述號碼處理部，其構成係在前述存儲信息區段資料含有複數之零件，使驗證對象之存儲信息零件有1個時，前述送驗證對象件被增強化時，藉由要驗證零件之譯碼處理將預取譯碼全文體以預定組元單位在進行譯碼處理和後之值，運用存儲信息核對值生成之後用以執行號碼處理並用以生成存儲信息核對值，使前述存儲區零件未被增強化時，將該圖驗證零件全體以異或之先單位將進行譯碼處理和後之值，運用前述存儲信息核對值生成論述用以執行號碼處理並用以生成存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述號碼處理部，其構成係在前述存儲信息區段資料含有複數之零件，使驗證對象之要驗證零件有複數時，在各零件適用存儲信息核對值生成論述用以執行號碼處理對對象之零件核對值的源碼資料，進而適用前述存儲信息核對值生成論述後用以執行號碼處理將所取得結果做為存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理部，係送函，在前述號碼處理部中具有記號數用以容納存儲信息資料並執行正當性驗證對象之存儲信息資料。

進而，本發明之資料處理方法之一實施態樣中，在前述

五、發明說明（<sup>45</sup>）

資料處理方法，其特徵為：係依據對象之存儲信息區段資料被增強化時，藉由要驗證信息區段資料之譯碼處理將預取譯碼全文體以預定組元單位進行號碼處理並用以生成存儲信息中間值，並驗證對象之存儲信息區段資料未被增強化時，將存儲信息區段資料全文體以預定組元單位進行號碼處理並用以生成存儲信息中間值。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：在前述中間值對值的生成論述並用前述論述定之論述依據依循性論述和單。

進而，本發明之資料處理方法之一實施態樣中，在前述存儲信息中間值之生成論述，其特徵為：係驗證對象之存儲信息同步資料被增強化時適用於存儲信息中間值生成論述並用前述論述處理，依據ABC模式之譯碼處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：藉由ABC模式之譯碼處理構成，係構成係在形成處理對象之信息列的一部分被適用複數次共同論述論述號處理。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：在存儲信息區段資料含有複數之零件，並使被合於該存儲信息區段資料一部分之零件有驗證對象時，根據驗證對象零件用以生成存儲信息核對值，並非用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之各存儲信息區段資料單位的正常性驗證處理。

五、發明說明（<sup>45</sup>）

前述號碼處理部中之存儲信息核對值的核對處理中，在尚未立核對後之情形，其特徵為：前述控制部，其構成係具有用以中止容納號碼對值記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理部，係送函，在前述號碼處理部具有再生處理部用以再容納執行正當性驗證對值之資料。

進而，本發明之資料處理方法之一實施態樣中，將該資料處理部，係送函，在前述號碼處理部中之存儲信息核對值的核對處理中，在未成立核對後之情形，其特徵為：前述控制部，其構成係具有在前述再生處理部用以中止再生處理。

進而，本發明之第2.2剖面。

係一種資料處理方法，藉由記錄譜體或訊訊系統進行被供應存儲信息資料處理的資料處理方法。

係在合於資料處理方法之一實施態樣中，而該資料處理部處理，其構成係在前述資料處理部並用以生成存儲信息核對值，藉由用以執行生成之後之存儲信息核對值之統計處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗證處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理部，係張譜體驗證對象之存儲信息區段資料並用以生成存儲信息中間值，並對生成之後之存儲信息中間值適用存儲信息核對值，並對成之後之存儲信息中間值用以生成存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，前述

五、發明說明（<sup>45</sup>）

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：在前述存儲信息同步資料被含有複數之零件，使驗證對象之要驗證零件有1個時，使前述號碼處理零件被增強化時，藉由要驗證零件之譯碼處理將取得譯碼全文體以預定組元單位在進行譯碼處理和後之值，運用存儲信息核對值生成論述後用以執行號碼處理並用以生成存儲信息核對值，使前述存儲信息核對值之增強化時，將該要驗證零件全體以預定組元單位將進行譯碼處理和後之值，適用前述存儲信息核對值生成論述用以執行號碼處理並用以生成存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：係在前述存儲信息同步資料被含有複數之零件，使驗證對象之要驗證零件有複數時，在各零件適用存儲信息核對值生成論述用以執行號碼處理對取得後之零件核對值的源碼資料，進而適用前述存儲信息核對值生成論述後用以執行號碼處理將取得結果做為存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係送函，而會被執行正當性驗證之後之存儲信息區段資料並用以容納存儲信息資料的步驟。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，係送函，在存儲信息核對值之核對處理中，在未成立核對後之情形，其特徵為：前述控制部，係用以中止容納號碼對值記錄裝置。

A7  
B7五、發明說明（<sup>48</sup>）

進而，本發明之資料處理方法之一實驗態樣中，其特徵為：前述存儲資料處理方法，係選用一存庫用以執行再生處理之資料應用以執行再生處理步驟。

進而，本發明之資料處理方法之一實驗態樣中，前述資料處理方法，係在存儲信息資料檢驗對象對應項中，在本成立後於其情形中，其特徵為：用以中止再生處理。

進而，本發明之第 2-3 頁面，係一種存儲信息資料檢驗賦予方法，為了存儲信息資料驗証之存儲信息資料檢驗賦予方法，其特徵為：在前述存儲信息資料檢驗對象之存儲信息資料單位用以生成存儲信息資料對象，並將生成之後之存儲信息資料對象結合驗証對象存儲信息資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗証賦予方法之一實驗態樣中，其特徵為：前述存儲信息資料對象，係將形成該對對象之存儲信息資料作為信息，適用存儲信息資料對象生成點藉由確認資訊被生成之值。

進而，本發明之存儲信息資料驗証賦予方法之一實驗態樣中，其特徵為：前述存儲信息資料對象，係根據驗証對象之存儲資料同步資料用以生成存儲信息中間值，對該存儲信息中間值選用前述存儲信息對象生成點後用以執行辨識兩項被生成之值。

進而，本發明之存儲信息資料驗証賦予方法之一實驗態樣中，其特徵為：前述存儲信息資料對象，係對驗証對象之存儲信息資料根據 C-B-C 構式藉由用以執行確認。

本紙張尺寸適用中國郵政標準 (CHS)A4 尺寸 (210×297 公釐) - 51-

A7  
B7五、發明說明（<sup>49</sup>）

處理被生成之値。

進而，本發明之存儲信息資料驗証賦予方法之一實驗態樣中，其特徵為：保在存儲信息區段資料被合有復數之零件，將被合於該存儲信息區段資料一端之零件用以驗証對象時，根據驗証對象零件用以生成存儲信息資料對象，並將生成之後之存儲信息直接對對象驗証對象存儲信息資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗証賦予方法之一實驗態樣中，其特徵為：在前述存儲信息區段資料被合有復數之零件，要驗証對象之要驗証零件有 1 個點，便前述要驗証零件被確認化時，藉由要驗証零件之譯碼處理將被取得譯碼與文字標以預定紀元單位在進行辨識後用以執行辨識兩項被生成之值，前述要驗証零件將被轉換為記號化時，請該要驗証零件主體以預定紀元單位將進行辨識後和後之值，適用前述存儲信息對象生成點藉由用以執行確認點或後用以生成存儲信息對象，再生後之存儲信息資料對象並用以生成存儲信息對象，再生後之存儲信息資料。

進而，本發明之存儲信息資料驗証賦予方法之一實驗態樣中，其特徵為：保在前述存儲信息同步資料被合有復數之零件，要驗証對象之要驗証零件有 1 個點，在各零點適用存儲信息直接生成論述所以執行確認或處理對象之後之零件被記憶的連結資料，進而適用前述存儲信息對象生成論述後用以執行確認或經並將最近存儲結果做為存儲

本紙張尺寸適用中國郵政標準 (CHS)A4 尺寸 (210×297 公釐) - 52-

A7  
B7五、發明說明（<sup>50</sup>）

信息對象後，再生後之存儲信息資料對象存儲信息同步資料賦予存儲信息資料。

進而，本發明之第 2-4 頁面。

係一種資料提供處理，用以提供兩組程式而由記憶與繼或追蹤資料將被提供存儲信息資料之處理在電腦系統上執行之程式供給軟體，其特徵為：前述存儲程式，係含有：於被合於資料結構對象之存儲資料同步資料單位用以生成存儲信息資料對象的步驟，及前述用以執行生成之後之存儲信息資料對象的辨別或值，用以執行前述資料中之存儲信息同步資料單位的正常性辨識處理之步驟。

進而，本發明之第 2-5 頁面。

係一種資料處理裝置，具有使至少一部分之資料被縮減化後之複數之存儲信息資料，及用以容納有關該存儲信息資料之資訊的集管部列於該存儲信息資料之記錄装置用以執行存儲資訊資料之處理的資料處理裝置。

前述該資料處理裝置，

係對前述記錄裝置使形成對象之存儲信息資料，前述存儲信息區段之存儲資料 Kds 藉由暗碼論匙 Kds 諸執行暗碼處理後之暗碼論匙資料 Kds (Kor) 產生並用於前述集管部後之資料被編成的備形中，其特徵在於其構成具有：

將前述暗碼論匙資料 Kds (Kos) 由前述集管部進行取出用以執行暗碼處理並用以生成譯碼資料 Kcon，而對該生成之後之譯碼資料 Kcon 用不同暗號論匙 Kstr 與用以執行暗碼處理，根據暗號論匙 Kstr 用以生成密號處理後之暗號論匙資料並用以執行容納到前述存儲信息資料之集管部的處理。

進而，本發明之第 2-7 頁面。

A7  
B7五、發明說明（<sup>51</sup>）

行暗號處理，根據暗號論匙 Kstr 用以生成暗號處理後之暗號論匙與該資料被用以執行容納到前述存儲信息資料之集管部的處理。

本發明之第 2-6 頁面。

係一種資料處理裝置，具有使至少一部分之資料被縮減化後之複數之存儲信息資料，及用以容納有關該存儲信息資料之資訊的集管部列於該存儲信息資料之記錄装置用以執行生成存儲信息資料之處理的資料處理裝置。

前述該資料處理裝置，

係對前述記錄裝置使被合於形成對象之存儲信息資料的前述存儲信息區段，藉由暗號論匙 Kdc 被縮減化後之存儲信息，及根據暗號論匙 Kcoa 與被縮減化後之暗號論匙資料 Koc (Kic) 被生成，進而，構成有將前述暗號論匙 Koc 與由暗號論匙 Kds 沒進行暗號處理後之暗號論匙資料 Kds (Kcon) 容納到前述集管部之情形中，其特徵在於其構成具有：

將前述暗號論匙資料 Kds (Kcon) 由前述集管部進行取出用以執行暗碼處理並用以生成譯碼資料 Kcon，而對該生成之後之譯碼資料 Kcon 用不同暗號論匙 Kstr 與用以執行暗碼處理，根據暗號論匙 Kstr 用以生成密號處理後之暗號論匙資料並用以執行容納到前述存儲信息資料之集管部的處理。

進而，本發明之第 2-7 頁面。

係一種資料處理裝置，具有使至少一部分之資料被縮





A7  
B7五、發明說明（<sup>90</sup>）

該存儲信息資料之真實資訊用以取得存儲信息資料之構成資訊並進行存儲信息資料之解析。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：在前述存儲資訊，係被合併而存儲信息之再生優先順位資訊，在前述存儲資訊中使彤序長處理對象之服務存儲信息有複數時，則前述彤序長處理部，係在前述存儲信息資料解析步驟並取得後之真實資訊中的優先級位資訊，依從該優先順位用以執行順序存儲信息彤序長之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係正面，具有：顯示裝置，用以顯示形或彤序長處理對象之服務存儲信息的資訊；及輸入裝置，由使用者於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息對象資訊；前述彤序長處理部，係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之服務存儲信息的彤序長處理之構成。

進而，本發明之第3.5剖面。

係一種資料處理裝置，而由記憶装置或訊訊媒體進行被提供之存儲信息資料的再生處理之資料處理裝置，其特徵在於：

用以接收含服務存儲信息，並伴長處理程式其中之一的存儲信息資料，由被合於接收存儲信息資料之黑管資訊並被存儲信息資料用以分別對應存儲信息彤序長處理程式

A7  
B7五、發明說明（<sup>81</sup>）

・當時

該存儲信息資料有服務存儲信息時，由該存儲信息資料之真實資訊，用以取勝被適用於該服務存儲信息後之服務處理程式獲致。

並具有：存儲信息資料解析部，使該存儲信息資料具有彤序長處理程式時，由該存儲信息資料之無害資訊用以取勝彤序長處理程式獲致；及

彤序長處理部，用以執行服務存儲信息之彤序長處理；

前述存儲信息資料解析部被解析後之服務存儲信息的服務處理程式獲致可適用之彤序長處理程式，藉由前述存儲信息資料解析部根據被解析後之彤序長處理程式之服務處理部選擇，藉由該選擇後之彤序長處理程式用以執行彤序長處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係正面，其構成具有：資料記憶部，由前述存儲信息資料解析部用以容納被抽出後之服務存儲信息；及程式記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之彤序長處理程式；而前述彤序長處理部，係對被記憶於前述資料記憶部後之服務存儲信息，適用被記憶於前述資料記憶部後之彤序長處理程式並用以彤序長處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：在前述存儲資訊，係被合併而存儲信息之再生優先順位資訊。

A7  
B7五、發明說明（<sup>62</sup>）

該位資訊，並形成彤序長處理對象之服務存儲信息有複數時，則在前述彤序長處理部之中存儲信息彤序長處理，係在前述存儲信息資料解析部中根據被取得後之真實資訊中的優先順位資訊，依從該優先順位進行順序執行之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，其具有檢索装置用以檢索彤序長處理程式，而前述檢索裝置，對該檢索前述存儲信息資料解析部後之再生存儲信息將可適用之彤序長處理程式，而前述資料處理裝置所可取收之程式資料檢索依據係被檢索對象進行順序之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵在於：

前述資料處理裝置，係正面，具有：顯示裝置，用以顯示形或彤序長處理對象之服務存儲信息的資訊；及輸入裝置，由使用者於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資訊；前述彤序長處理部，係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之服務存儲信息的彤序長處理之構成。

進而，本發明之第3.7剖面。

係一種資料處理方法，係合記憶體或訊訊媒體進行被提供之存儲信息資料的再生處理之資料處理方法，其特徵係具有：

存儲信息資料解析步驟，合記憶體後之存儲信息及該

A7  
B7五、發明說明（<sup>63</sup>）

服務存儲信息之彤序長處理程式用以執行存儲信息資料之存儲信息資料剖析，並用以執行由該存儲信息資料之服務存儲信息，及彤序長處理程式之抽出處理；及

彤序長處理部，做為前述存儲信息資料解析步驟之後之彤序長處理程式，藉由前述存儲信息資料之彤序長處理程式用以執行被合於該服務存儲信息之存儲信息資料之彤序長處理程式用以執行存儲信息資料之服務存儲信息的彤序長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理裝置，其成構係進而具有：資料記憶步驟，藉由前述存儲信息資料解析步驟用以容納被抽出後之服務存儲信息；及程式記憶步驟，藉由前述存儲信息資料之彤序長處理程式用以容納被抽出後之彤序長處理程式；而前述彤序長處理步驟，係對被記憶於前述資料記憶步驟後之服務存儲信息，在前述資料記憶步驟後之彤序長處理步驟中適用被記憶後之彤序長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述無害資訊，係被合記憶體後之再生優先順位資訊，在前述彤序長處理部中使彤序長處理對象之服務存儲信息有複數時，則前述彤序長處理步驟，係在前述存儲信息資料解析步驟中根據被取得後之真實資訊中的優先

A7  
B7

## 五、發明說明 (64)

類位資訊，依從該優先順位用以執行順序存儲信息仲長處理，

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係通過，具有：顯示步驟，將形成仲長處理對象之歷程存儲信息的資訊顯示於顯示裝置；及輸入步驟，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入甚麼選擇之後之再生存儲信息資料；而前述仲長處理步驟，係在前述輸入多個資訊被輸入之後之再生存儲信息資料並資訊，用以執行對應於該歷程資料之歷程存儲信息的仲長處理。

更而，本發明之第 3 例側面。

係一圖實利處理方法，藉由記憶媒體或遠訊媒體進行被提供之存儲信息資料的再生處理之資料處理方法，其特徵在於：

用以接收合歷程存儲信息，或於存儲過程其中之一的再生存儲信息資料，由被合的接收者存儲信息資料的集管資訊使用該存儲信息資料用以执行仲長處理前存儲信息或仲長處理程式，同時。

而該存儲信息資料有歷程存儲信息時，由該存儲信息資料之真實資訊，用以取得被被該歷程存儲信息後之歷程處理程式，並真有：

存儲信息資料解說步驟，而該存儲信息資料有仲長處理程式時，由該存儲信息資料之真實資訊用以取得仲長處理程式。

本版權及專利申請書件(CN104444684)第6頁(238+207公頁) - 67 -

A7  
B7

## 五、發明說明 (65)

長處理程式，將可存取之歷程資料並根據再檢索對象進行檢索，

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係通過，具有：顯示步驟，將形成仲長處理對象之歷程存儲信息的資訊顯示於顯示裝置；及輸入多個，由被顯示於前述顯示裝置後之存儲信息資訊用以輸入甚麼選擇之後之再生存儲信息資料；而前述仲長處理步驟，係由前述輸入多個資訊被輸入之後之再生存儲信息資料，用以執行對應於該歷程資料之歷程存儲信息的仲長處理。

更而，本發明之第 3 例側面。

係一存儲信息資料生成方法，藉由記憶媒體或遠訊媒體進行被提供之存儲信息資料的生成處置之存儲信息資料生成方法，其特徵為：

用以生成使歷程相後之存儲信息及該歷程在記憶體之仲長處理程式組合的存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，並無其特徵為：做為前述存儲信息資料之真實資訊用以附加該存儲信息資料之稱資訊。

進而，本發明之存儲信息資料生成方法之一實施態樣中，並無其特徵為：做為前述存儲信息資料之真實資訊，係用以附加被結合於該存儲信息資料之存儲信息之再生優先順位資訊。

進而，本發明之第 4 0 頁面。

本版權及專利申請書件(CN104444684)第7頁(238+207公頁) - 69 -

A7  
B7

## 五、發明說明 (65)

運算步驟，在前述存儲信息資料解析步驟中對分析後之歷程存儲信息的歷程處理程式種類將可適用之仲長處理程式，藉由前述存儲信息資料解析步驟根據被解析後之仲長處理程式種類加以選擇；及

仲長處理步驟，在前述選擇步驟中藉由選擇後之仲長處理程式用以執行仲長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係通過，具有：資料記錄步驟，藉由前述存儲信息資料解析步驟用以容納並抽出後之歷程存儲信息；及程式記錄步驟，藉由前述存儲信息資料解析步驟用以容納並抽出後之仲長處理程式；而前述作為處理步驟，係在前述資料記錄步驟後被記憶後之仲長處理步驟中，並前述資料記錄步驟後被記憶後之仲長處理程式用以仲長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：在前述萬能資訊，係包含歷程存儲信息之再生優先順位資訊，並形成仲長處理對象之歷程存儲信息有複數選擇，則在前述仲長處理步驟，係在前述存儲信息資料解析步驟中根據被取得後之萬能資訊中的優先順位資訊，依從該優先順位進行順序執行。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係通過，具有被檢索步驟用以檢索仲長處理程式，而前述檢索步驟，在前述存儲信息資料解析步驟中對進行解析後之歷程存儲信息種類將可適用之仲長處理。

本版權及專利申請書件(CN104444684)第8頁(238+207公頁) - 68 -

A7  
B7

## 五、發明說明 (67)

係一歷程存儲信息資料生成方法，藉由記憶媒體或遠訊媒體進行被提供之存儲信息資料的生成處理之存儲信息資料生成方法，其特徵為：

使存儲信息資料用以識別該歷程存儲信息或仲長處理程式之存儲信息資料編碼為萬能資訊並進行附加。

使該存儲信息資料係配給存儲信息，則將被適用於該編碼存儲信息後之歷程處理程式種類為萬能資訊並進行附加。

而使該存儲信息資料係仲長處理程式時，則將仲長處理程式種類做為萬能資訊並用以生成附加後之存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：啟動的該存儲信息資料之真實資訊，係用以附加結合於該存儲信息資料之存儲信息的再生優先順位資訊。

進而，本發明之第 4 1 頁面。

係一種程式提供媒體，用以提供電腦程式藉由記憶媒體或遠訊媒體被提供存儲信息資料之再生處理在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，其特徵具有：

存儲信息資料解析步驟，被被歷程後之存儲信息及該歷程存儲信息之仲長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之歷程存儲信息，及仲長處理程式之拍出處理；及

本版權及專利申請書件(CN104444684)第9頁(238+207公頁) - 70 -

AT  
BT**五、發明說明 (66)**

仲共處理步驟，做為前述存儲信息資料解說之分析結果來使用當有被啟後之存儲信息資料的仲共處理程式用以執行被包含於該存儲信息資料之整體存儲信息的仲共處理。

有甚本發明之程式提供媒體，係舉如，兩種種之程式代碼對可執行的浪用電腦系統，將電腦程式以電動可讀之形式進行操作之媒體，依據，係 C D 或 F D 、 M O 等之記憶媒體，或，網路等之傳送媒體等，其形態並無特別限定。

如此之程式提供媒體，係在電腦系統上為了用以實現預定之電腦程式的功能，用以定義電腦程式及提供媒體之傳送或功能上協助性關係，換言之，透過該提供媒體新電腦程式由受制於電腦系統，在電腦系統上被發揮協助性作用，可取得原本發明其他與之同樣的作用效果。

本發明實施例與其他目的，竹微或便貼，係根據後述之本發明實施例與後述圖之說明為更明確吧！

**【發明之實施形態】**

以下用以說明本發明之實施形態，說明之順序，係根據以下之項目進行。

- (1) 實質處理與實質成
- (2) 存儲信息資料形式
- (3) 實質處理裝置中之可適用的記憶處理概念
- (4) 記錄再生器之零納資料構成

本領域人民適用中國國家標準 (CNISDA44 國標 (210+297 公量) - 71 -

AT  
BT**五、發明說明 (70)**

3 0 0 及記錄裝置 4 0 0 做為主要構成要素。

記錄再生器 3 0 0 ，係譽如釋由個人電腦 ( P C : Personal Computer ) 、或遊戲機器等構成，記錄再生器 3 0 0 ，係如圖 2 所示，具有：控制部 3 0 1 、用以執行總性質之控制再生器 3 0 0 中內部處理時之記錄裝置 4 0 0 的選項控制；記錄再生器 3 0 0 上被稱為處理部 3 0 2 、音處理裝置全體；記錄裝置控制部 3 0 3 、被述於記錄再生器 4 0 0 用以執行記錄並並進行資料之廣出；顯示部 3 0 4 、由 D V D 等之媒體至進行資料之廣出；及選訊部 3 0 5 、與內部進行資料之收發。

記錄再生器 3 0 0 ，係譽由控制部 3 0 1 之控制對記錄裝置 4 0 0 之存儲信息資料之下，由記錄裝置 4 0 0 用以執行存儲信息資料和再生。記錄裝置 4 0 0 ，係於記錄再生器 3 0 0 機体内可识别之記錄媒體，譬如記憶卡等，具有外部記憶體 4 0 0 2 由 E E P R O M 、閃光記憶體等之非易失記憶體，硬碟、附屬池 R A M 等被構成。

記錄再生器 3 0 0 ，係具有：選訊部 3 0 4 、將並容許於圖 2 之左端所示之記憶媒體、 D V D 、 C D 、 F D 、 H D D 後之存儲信息資料做為可插入；及選訊部 3 0 5 、由資訊測頭等之術語並記訊將存儲信息資料做為可輸入的接口；由外部用以輸入存儲信息。

記錄再生器 3 0 0 ，係具有：總號處理部 3 0 2 、通過選訊部 3 0 4 或選訊部 3 0 5 將由外部被輸入之存儲信息資料在記錄裝置 4 0 0 進行下載或上傳，或將存儲信息資

AT  
BT**五、發明說明 (69)**

(5) 記錄裝置之零納資料構成

(6) 記錄再生器、記錄裝置間中之相互認証處理

(6-1) 相互認証時之摘要

(6-2) 相互認証時之摘要與密鑰的切換

(7) 由記錄再生器到記錄裝置之下載或上傳

(8) 以紀錄與存儲客資資訊之記錄再生器的再生處理

(9) 相互認証時之鍵匙交換處理

(10) 讀數之存儲信息資料形式，及對應於各形式之下載或再生處理

(11) 存儲信息供應者中之核對值 ( I C V ) 生成處理模組

(12) 核對主據點之所著或推論之生成與成

(13) 處理過程中之所著強制抑制

(14) 授權存儲信息資料中之處理力計中的啓動優先級位之程式啓動處理

(15) 存儲信息構成及再生 ( 伸縮 ) 處理

(16) 存儲資料之生成以及對記憶裝置的容納，再生處理

(17) 不正確機器之防護結構

(18) 安全晶片構成及製造方法

**(1) 實質處理從屬構成**

圖 2 係顯示有甚本發明之實質處理裝置之一實質剝離器成方塊圖。本發明之資料處理裝置，係若記錄再生器

本領域人民適用中國國家標準 (CNISDA44 國標 (210+297 公量) - 72 -

AT  
BT**五、發明說明 (71)**

藉由記錄裝置 4 0 0 再生，進行執行將之擴張處理，增強化處理，譯碼化處理，進而用以執行資料之驗證處理等，增強處理部 3 0 2 其構成詳真有：控制部 3 0 0 用以控制增強處理部 3 0 2 ；內部記憶體 3 0 7 、用以保持增強處理部 3 0 2 等的資訊，並由外部被輸入不容易使資料譯出之處理；及增強 / 譯碼化部 3 0 8 、進行增強化處理，譯碼化處理，經此用之資料的產生，數數之產生等。

控制部 3 0 1 、係譽在，記錄再生器 3 0 0 搭載著記錄裝置 4 0 0 時透過記錄裝置控制器 3 0 3 發送切勿化指令到記錄裝置 4 0 0 ，或，在記錄再生器 3 0 0 與處理部 3 0 2 之間把 / 譯碼化部 4 0 8 之間進行在相互交叉處理，根據控制器對擴張，增強，譯碼化處理等，在各種處理中進行仲介處理。對於此等各處理，在後段加以詳細說明。

增強處理部 3 0 2 ，係於前述用以執行記錄媒體，增強化處理，譯碼化處理，並對資料之驗証處理等之譯碼化，且具備記憶體控制器部 3 0 6 、內部記憶體 3 0 7 ，帶被 / 譯碼化部 3 0 8 。

增強處理控制器部 3 0 6 ，係在記錄再生器 3 0 0 中被執行者據認証處理，增強 / 譯碼化處理等之增強處理上面以執行控制之控制器。譬如，在記錄再生器 3 0 0 及記錄裝置 4 0 0 之間被執行在認證處理之終了時的，將被將了標記之設定，記錄再生器控制器部 3 0 2 之標記 / 譯碼化部 3 0 8 中被執行各種處理，譬如下載，或有甚再生

本領域人民適用中國國家標準 (CNISDA44 國標 (210+297 公量) - 73 -

A7  
B7

## 五、發明說明 (72)

存儲備份資料之核對值生成處理之執行指令，各種檢測之生成處理的執行指令等，進行有解碼號或處理全面的控制。

內部記憶體 307，係在後段加以詳述說明，但在記錄再生器 3000 之執行相互通訊處，依對核對對處理，縮小化，詳述化，譯碼化處理等，在各種處理形成必要之操作資料，或用以容納策劃資料等。

總覽／譯碼化即 308，係使用並容納於內部記憶體 307 後之論點資料等，由外部輸入將存儲備份資料在記錄再生器 4000 進行下載或複寫，或被寄存於記錄裝置 4000 之後存儲信息資料由記錄裝置 4000 進行再生，執行跨文件處理，縮小化處理，譯碼化處理，並應用以執行預定之核對值或電子簽名之生成，驗證，資料之驗証，亂數之產生等的處理。

對於，記錄再生器或處理器 302 之內部記憶體 307，係為了用以保持筆跡錄影等之重要之資訊，敘述由外部必要藉以不正常擋出之機制，因此，縮小化內部 302，係由外部以持有經由存取存儲之半導體晶片結構成，具備多層構造，其內部記憶體係依存於晶片之結構，或，在此之下單層構成，又，進行動作之處理或／及核對率之真確執事等，由外部具有難以不正常實質擋出之特性係以相應之記憶體結構成，對於該構成，係在後段加以詳細說明。

記錄再生器 3000，係除了此等之聯繫處理功能之外，且具有：中央演算處理裝置（主 CPU：Central

本說明文適用中國專利法規 (CN1044 號令) 第 102-207 (公量) - 76-

A7  
B7

## 五、發明說明 (73)

Processing Unit) 106 · RAM (Random Access Memory) 107 · ROM (Read Only Memory) 108 · A/V 段理部 109 · 輸入接口 110 · P10 (主端口 1 / O 接口) 111 · S10 (串列 1 / O 接口) 112 ·

中央演算處理裝置（主 CPU：Central Processing Unit）106 · RAM (Random Access Memory) 107 · ROM (Read Only Memory) 108，係為紀錄再生器 3000 之控制系統發揮功用之構成部，主要以記錄再生器號碼處理部 302 用以執行接譯而後之資料再生係為再生處理部發揮功能。譬如中央演算處理裝置（主 CPU：Central Processing Unit）106 · 係在控制部 301 之控制下由記錄裝置將被譯出接譯而後之存儲信息資料進行輸出到主 A/V 段理部 109 等，進行有關存儲備份之再生，執行之控制。

RAM 107，係為為 CPU 106 中之各種處理用之主記憶體擴充使用，係由 CPU 106 所有之處理數為作業領域而使用，ROM 108，所以主 CPU 106 被應用為丁了上列之 S 等被容的基本程式等。

A/V 處理部 109，具體而言，係認為具有 MPEG 2 淨碼器，ATRAC 說明器，MP3 淨碼器等之資料壓縮伸長處理模塊，對付單於記錄再生器並運後之朱漢式顯示器或接收器等之資料輸出機器用以執行得之資料輸出之處理。

輸入接口 110，係由接連接後之控制器，鍵盤，滑

本說明文適用中國專利法規 (CN1044 號令) 第 102-207 (公量) - 76-

A7  
B7

## 五、發明說明 (74)

皇帝，各項之輸入裝置所輸入資料輸出到主 CPU 106 · 主 CPU 106，係當如根據執行中之遊戲程式等由使用者指揮控制係依指示而執行處理。

P10 (並聯 1 / O 接口) 111 · S10 (串列 1 / O 接口) 112 · 弦列記憶卡 · 遊戲子匣等之記憶裝置 · 讀帶用電子機器等做為直接接頭之接頭用。

又，主 CPU 106，係當如若有所執行中之遊戲等設定資料等做為安全資料記憶在記錄裝置 4000 之時也進行控制，在該處理時，係將記錄資料轉送到控制部 301 · 控制部 301 係根據必要在該資訊處理部 302 有關係安全之外之增雙處理被執行，並將增雙化資料容納於記錄裝置 4000 · 對於此等之相應或處理，係在後段加以詳細說明。

記錄裝置 4000 · 係由前段所述係記錄再生器 3000 可與即之記憶裝置，譬如由記憶卡被構成，記錄裝置 4000 係具有增雙處理部 401 · 外部記憶體

記錄與增雙處理部 401，係由記錄再生器 3000 之存儲備份資料的下系，或由記錄裝置 4000 記錄再生器 3000 之存儲備份資料的再生處理時等中之記錄再生器 3000 及記錄裝置 4000 之間的相互認證處理，縮小化處理，詳述化處理，並應用以執行資訊之驗証或處理等的處理部 · 記錄再生器 3000 之增雙處理部 401 係有同樣控制部，內部記憶體，映射／譯碼化部等，等等之詳情係顯示於圖 3 · 外部記憶體 402，係如前述，譬如由 EEPROM 等

A7  
B7

## 五、發明說明 (75)

之閃光記憶體所構成非晶失火機體，藉由碟體，附電池 RAM 等被構成，並用以容納被標號化後之存儲信息資料。

圖 3 係顯示本發明之資料處理裝置由接收資料供給之存儲信息並提供其之記錄裝置 500 · 這訊息裝置 500 被輸入之資料構成包括筆記，同時由此等存儲信息供給裝置 500 · 600 所以輸入存儲信息將有記錄再生器 3000 · 及記錄裝置 4000 中之增雙處理的構成故為中心，顯示其機能或圖面。

裝置 500，係當如光纖傳輸，扭轉長臂，扭轉裝置，半導體探測等，通訊裝置 600，係應用網路將訊息，電視訊息，黑點訊訊等，可資料訊送之裝置。

圖 3 中，記錄再生器 3000，係由存儲信息提供裝置之記錄 500 · 通訊裝置 600 並輸入之資料，即如圖 3 所示係從接走之形式用以驗証存儲信息，並在驗証後將存儲信息保存於記憶裝置 4000 ·

知識 3 之記錄 5000 · 通訊裝置 600 部分所示存儲信息資料具有如下之構成部，具有：

識別資訊：做為存儲信息資料之識別資訊。

處理能力：存儲信息資料之構成資訊，譬如用以構成存儲信息資料之集散部所構成，存儲信息表格格式，形式之方式，存儲信息顯示程式或資料之存儲模式，並使存儲信息包含僅以下載後之機器可利用或以其他機器也可利用等之服務利用資訊等之處理方針。

本說明文適用中國專利法規 (CN1044 號令) 第 102-207 (公量) - 76-

本說明文適用中國專利法規 (CN1044 號令) 第 102-207 (公量) - 76-

A7  
B7

## 五、發明說明 (78)

區分資訊：由顯示存儲信息區段數，區段規格，暗號化之有無等資訊等被構成之區段資訊。

鑄記資料：由用以暗號化區段資訊之暗號化論述，或用以暗號化存儲信息區段之存儲信息指標等所構成之鑄記資料。

存儲信息資料：由形成實際之再生對象的程式資料，音頻，圖像資料所成存儲信息資料。

尚有：對於存儲信息資料之詳情，係在後段使用圖4以下述詳細加以說明。

存儲信息資料，係藉由存儲信息鑑匙（於此，係將此稱為存儲信息鑑匙（Content Key（以下，做Keen）））並暗號化，由記錄5000，資訊部4000者提供到記錄再生器3000，存儲信息，並透過記錄再生器3000可密納於記錄裝置4000之外部記憶體。

譬如：記錄裝置4000，係用該啟動號於記錄裝置內之內部記憶體4000之後之記錄裝置而有鑑匙（於此，係將此稱為存儲鑑匙（Storage Key（以下，做Kstr））），該含於存儲信息資料之存儲信息，及欲存儲信息資料之集集管識者皆有之區段資訊，各項錄音資訊，實如用以暗號化存儲信息鑑匙 Keen 者進行記錄於外部記錄裝置4000，由存儲信息資料之記錄再生器3000下載或傳到記錄裝置4000，或藉由記錄再生器3000被密納於記錄裝置4000內之存儲信息資料的再生過程中，使供檢閱而之相互認定處理，存儲信息資料之暗號化，譯碼化處理等，形

A7  
B7

## 五、發明說明 (77)

或必要設定之手續。對於此等之處理，係在後段加以詳細說明。

記錄裝置4000，係如圖3所示具有暗號處理部4001，外部記憶體402，西摩茲處理部401，低真音部403，邏輯部404，內部記錄裝置405，暗號／譯碼化部406，及外部記錄體控制部407。

記錄裝置4000，係當其非正常處理全面，用以預計外部記錄裝置402，同時由記錄再生器3000用以解釋指令，由用以執行或記錄資訊處理等處理部401，及用以保持存儲信息等之外部記錄裝置402所構成。

記錄裝置密納於處理部401，係具有：控制部403，用以控制記錄裝置或處理部401之全體，資訊部404，與記錄再生器3000進行資料之收發；內部記錄裝置405，用以保持記錄裝置之維持資料等之資訊，並由外部都不容易識出其真實處理；暗號／譯碼化部406，進行暗號化處理，譯碼化處理，將註冊之資料之生成，破譯，亂數之產生等；及外部記錄體控制部407，用以達到外部記錄裝置402之資料。

控制部403，係在記錄裝置4000中用以執行有權被執行之認證處理，暗號化／譯碼化處理等之暗號處理全體的監制部，譬如，在記錄再生器3000及記錄裝置4000之間被執行之認證處理終了時之認證終了標記之發生，確為處理部401之增強／譯碼化部406半之被執行的各種處理。譬如下載，或有解再生存儲信息資料之係

本說明文書所用語彙參照(CNSI)A規範(120×207公厘) - 79 -

A7  
B7

## 五、發明說明 (78)

對產生成處理之執行命令，各種鑑匙資料之生成處理的執行指令等，進行有權密納而形成全面之控制。

內部記錄裝置4005，係在記錄裝置說明，但藉由元件構成而記錄裝置被構成，在記錄裝置4000中被執行之存儲記憶處理，核對值嵌入處理，暗號化，譯碼化或亂數等，在各種處理而形成必要之鑄記資訊，或形成用以存放數字的異別資料等組成之構成。

記錄裝置等處理部401之內部記錄裝置405，係與前面說明之記錄再生器3002之內部記錄裝置3007不同，為了用以保存記錄裝置等之重要資訊，由外部而有其異形或難以不正當而提出之構造。因此，記錄裝置4000之說明處理部401，係由外部而有其難以存取機器之特殊構造品被構成，其內部之記錄裝置等之記錄裝置等之複雜，被結構於最下層，又，使動作之複雜度／且複雜之異質罕有，被構成為由外部難以不正當資訊提出之特性。尚有：記錄再生器號碼處理部3002，係將諸多等之秘密資訊不密納到外部被構成之狀態也可。

暗號／譯碼化部406，係由記錄再生器3000之存儲信息資料的下載處理，被密納於記錄裝置4000之外部記錄裝置4002之後之存儲信息資料的再生處理，或記錄再生器3000及記錄裝置4000之間相互認定處理時，用以被密納於內部記錄裝置4005之後之鑄記資訊等，用以執行資料之認證處理，暗號化處理，譯碼化處理，預定之核對值或

A7  
B7

## 五、發明說明 (79)

電子簽名的生成，驗証亂點之產生等的處理等。

資訊部404，係被選取記錄再生器3000之記錄裝置控制部3003，係從記錄再生器3000之記錄部3001，或記錄裝置4000之記錄部4003，進行存儲信息資料之下載處理，再生，或刪，或，相互通認處理等之記錄再生器3000及記錄裝置4000間的傳送資料之資訊。

## (2) 存儲信息資料格式

其次，使用圖4乃至圖6，對於被密納於水發明之系統中之錄音5000，或用以流傳資料送訊裝置800之資料格式說明。

圖4所示之構成係顯示存儲信息資料生體之格式圖，圖5所示之構成係顯示以構成存儲信息資料之無管部的一部分「區域分割」之詳細圖，圖6所示之構成係顯示用以構成存儲信息資料之無管部的一部分「區域資訊」之詳細圖。

尚有，於此，係對於本發明系統中被應用之資料格式之代表性的二例加以說明。但本發明之系統，係採用根據於錄取程式之格式，適用於音頻資料等之實時處理的格式等，使不同種數之資料格式可利用，對於此等之格式的選擇，係在後段「(1) 上復數之存儲信息資料格式，及對於各模式之下載及再生處理」中，更詳細述。

圖4所示資料格式中，以灰色顯示部分係被暗號化之後之資料，二重框部分係改核對資料，其他之白色部分係

本說明文書所用語彙參照(CNSI)A規範(120×207公厘) - 81 -

本說明文書所用語彙參照(CNSI)A規範(120×207公厘) - 82 -

A7  
B7

## 五、發明說明 (80)

未被編號化平臺之資料，經試驗認定其辨識化論述，係分別顯示於右之左邊之論述。第 4 所示例中，係在存儲信息區段之各區段（存儲信息區段資訊）而在有被暗號化之區段及未被暗號化之區段。此等之情形，係根據存儲信息資料不同的情形，使基於於實質全部之存儲信息區段資料被暗號化的論述也可。

如圖 4 所示，資料格式，係分成集散部及存儲信息區，集散部，係藉由資訊資訊（Content ID），處理方針（Usage Policy），絕對值 A（Integrity Check Value A（以下，簡稱為 I C V a）），區段資訊鍵（Block Information Table Key（以下，簡稱為 Kbit）），存儲信息論述 Kcon，並段資訊（Block Information Table（以下，簡稱為 B I T）），校對值 B（I C V b）達成對（I C V t）被構成，而存儲信息區段，係由總數之存儲信息區段（譬如說轉換後之存儲信息，及本被暗號化之存儲信息）被構成。

於此，詳列資訊，係顯示為用以識別存儲信息之資訊指標子（Content ID），處理方針，係如圖 5 所示之詳情，由顯示集散部分之大小的集散大小（Header Length），顯示存儲信息部分之大小的存儲信息大小（Content Length），顯示格式之方式資訊的格式版本（Format Version），顯示格式之類型的格式型態（Format Type），顯示被選擇存儲信息之存儲信息存儲程式，或資料等級存儲信息之類型的存儲信息類型（Content Type），存儲

專利申請書專題之說明文字

本辦法及規則中所指之公分 (CNS) A 級別 (220×220 公分) - 63 -

(內容說明文字之說明文字)

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

A7  
B7

## 五、發明說明 (82)

資訊匙 Kcon，係用以暗號化存儲信息區段而被使用，尚有，資料區段資訊匙 Kbit 及存儲信息匙 Kcon，係在具體 500 上下及資訊鍵度 6 00 上依後述之把記錄（Encryption Key（以下，簡稱為 Kbit））被逕能化。

將前述資訊之詳情顯示於圖 6，尚有，圖 6 之區段資訊，係如圖 4 資訊解釋為全部資料區段資訊匙 Kbit 被逕能化之資料，區段資訊，係如圖 6 所示，由顯示存儲信息區段之數的存儲信息區段（Block Number）及 N 位之存儲信息區段資訊匙擴張成，存儲之資訊資訊，係由區段大小（Block Length），顯示是否被暗號化之暗號化標記（Encryption Flag），顯示是否有必要用以計算校對值之始証對象匙（ICV Flag），存儲信息校對值（I C V t）被構成。

存儲信息校對值，係為了用以驗證各存儲信息區段之算校被應用之核對值，對於存儲信息校對值之生成方法的具體例，係在後述「(10) 資料之資料格式，及對應於各格式之下載處理對記錄資訊及由記錄資訊之再生處理」之闡釋加以說明，尚有，將區段資訊匙進行其資料區段資訊匙 Kbit，係存儲，藉由前述論述 Kbit 被暗號化。

繼續圖 4 之資料格式的說明，核對值 B、I C V b，及 I C V t，係為了用以驗正當設資訊匙 Kbit，及存儲信息匙 Kcon，區段資訊匙之算校的核對值，並存儲信息資料全體而係部分資料之核對值，即做為部分核對值發揮功能，總核對值 I C V t，係為了用以算校 I C V a、I C V b，名存

(內容說明文字之說明文字)

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

專利申請書專題之說明文字

本辦法及規則中所指之公分 (CNS) A 級別 (220×220 公分) - 65 -

A7  
B7

## 五、發明說明 (83)

信息匙區段示程式時之啓動優先順位的啓動優先順位資訊（Operation Priority），係依該格式使被下載後之存儲信息，僅能利用下載該之機器，或顯示可利用其他同樣機器的限制利用資訊（Localization Field），係依該格式使基於下載後之存儲信息，顯示由下載後之後是否在其餘是否在其餘同樣的機器可啓動之移動限制資訊（Move Permission），或顯示該格式化存儲信息部之存儲信息是否基於而顯示使用之算法的暗號算法（Encryption Algorithm），用以暗號化存儲信息部之存儲信息區段而顯示使用之算法的使用方法之暗號化模式（Encryption Mode），顯示核對值之生成方法的暗號方法（Integrity Check Method）被構成。

所有，記錄於上述之處理方針的資料項目，係 1 項之例，據對應之存儲信息資料的想樣可用以記錄種種之處理方針資訊，並要在記錄之「(17) 不正當機器之排除機制」加以詳細說明，惟不正當之記錄再生器的識別子進行記錄，藉由限制開始將之核對由於不正當機器耗用以存儲存儲信息利用之構成也可。

據對應 A、I C V a，係為了用以啟動資訊資訊，處理方針之默收的機制，並非存儲信息資料全體而供部分資料之核對值，即兩兩部分核對值發揮功能，資料級級資訊匙為 Kbit，係用以暗號化區段資訊而存儲而使用，而存儲信

本辦法及規則中所指之公分 (CNS) A 級別 (220×220 公分) - 64 -

A7  
B7

## 五、發明說明 (83)

信息匙區段之核對值 I C V t（被設定之情形），此等之部分核對值，或成其核對對象之資料全部的核對值。

尚有，將 6 中，將存儲大小，暗號化標記，驗證對參標記以由可設定，但假若某程度規則則成也可，譬如，將括號式文標記及平常文標記進行重複固定大小，或將全存儲信息行暗號化，用以壓縮區段資訊匙 I T 可以，又，存儲資訊資料匙 Kcon 在各存儲信息區段爲了形成不同，存儲信息匙匙 Kcon 并非在黑單部分，使於存儲信息區段也可。對於存儲信息資料之例，係在「(10) 暗號化之存儲信息資料格式，及對應於各格式下載及再生處理」之項目中，加以詳細說明。

## (3) 本發明之資料處理裝置中可適用之暗號概要

其次，對於本說明之資料處理裝置中被適用取得之各權限號碼的無效性加以說明，尚有，有權顯示於本項目「(3) 本發明之資料處理裝置中可適用之暗號處理之核對值」之暗號處理的說明，係在後段以具體加以說明未發明之資料處理裝置中之各項處理，譬如 a、記錄再者之記錄裝置間之認證處理，b、對存儲信息之記錄裝置的下載處理，c、容納於紀錄裝置後之存儲信息的再生處理等處理中對於被執行形反應與認證處之暗號處理的無效性，將其概要加以說明，對於記錄再者之記錄裝置 4 00 中之具體性處理，係在本說明書之項目「(4)」以下，對各處理詳細加以說明。

專利申請書專題之說明文字

本辦法及規則中所指之公分 (CNS) A 級別 (220×220 公分) - 65 -

（專利申請書專題之說明文字）  
裝（專利申請書專題之說明文字）  
裝（專利申請書專題之說明文字）  
裝



五、發明說明 (88)  
Hash (M)。

於此，使用亂數函數將求出亂數值方法加以說明，所調亂數函數，係將信息値作為輸入，並將此壓縮成預定之位元長的資訊，做為亂數值進行輸出之函數。亂數函數，係由亂數值（輸出）用以預測輸入為困難，並使輸入於亂數函數後之資料的 1 位元進行變化等，使亂數值之多位元產生變化，又，具有找出與有同一亂數值不同的輸入資料為困難之特徵。做為亂數函數，也有很使用 MD-4，MD-5，SHA-1 等的情形。該情形，係使形成最後輸出值 MAC ( 核對值：相當於 I C V ) 成為亂數值。

接著，在步驟 S 3，所以生成亂數  $u$  ( $0 < u < r$ )，並在步驟 S 3 將基點用以計算進行  $u$  值後之座標  $V$  ( $X_v, Y_v$ )。而有，隨即由線上之加減， $2$  值算值如下被定義。

【註 1】

$$\text{做為 } P = (X_a, Y_a), Q = (X_b, Y_b), R = (X_c, Y_c) = P + Q$$

$P + Q$  的 (計算)

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_b) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P + Q$  的 (2 倍算)

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

五、發明說明 (88)

算信息 M 之亂數值，做為  $f = \text{Hash} (M)$ 。其次，在步驟 S 1.4 用以計算  $h = l / d \bmod r$ ，並在步驟 S 1.5 所以計算  $h_1 = f \cdot h \bmod r \cdot h_2 = c$   $h \bmod r$ 。

在步驟 S 1.6 中，使用已述計算之  $h_1$  及  $h_2$ ，用以計算  $r - (X_p, Y_p) = h_1 \times G + h_2 \cdot K_s \times G$ ，電子簽名驗證者，係已如有公開編碼 G 及  $K_s \times G$ ，所以與步驟 1.1 之步驟 S 4 同樣可計算兩側曲線上之點的組合，而且，在步驟 S 1.7 用以判斷點 P 是否無限遠點，若非無限遠點則到步驟 S 2.0，若為無限遠點則到步驟 S 1.6 之進行。總之，進行  $F = (X, Y) \cdot Q = (X, -Y)$  之計算，則使 A 不能計算，何明  $F + Q$  在無限遠點。在步驟 S 1.8 用以計算  $p \bmod r$ ，並與電子簽名資料進行比較。在此後，則到步驟 S 1.9，判定電子簽名係正確時，則進到步驟 S 1.9，判定電子簽名係正確時。

判別此電子簽名係正確時，資料係不被篡改，可如何以保持對應於公開編號之密鑰編號者用以生成電子簽名。

在步驟 S 1.2 中，使電子簽名資料 c 或 d，未滿足  $0 < c < r$ ， $0 < d < r$  時，則進到步驟 S 2.0。又，在步驟 S 1.7 中，點 P 在無限遠點時也進到步驟 S 2.0。進而又，在步驟 S 1.8 中，使  $X_p \bmod r$  之值，未與電子簽名資料 c 一致時也進到步驟 S 2.0。

在步驟 S 2.0 中，被判定電子簽名不正確時，資料係

五、發明說明 (88)

$$x = (3 \cdot (X_a)^k + a) / (2 \cdot Y_a)$$

使用此等用以計算 G 之 u 值（速度慢，但較為容易了解之演算方法如下進行）。用以計算  $G \cdot 2 \times G \cdot 4 \times G \cdots$ ，將 u 進行 2 進位數展開用以算其對應於使 1 成立時之  $2^i \times G$  (將 G 進行 1 次 2 進算之倍) (( 係由  $u \geq L \cdot S \cdot B$  故時之完全位值 ))。

在步驟 S 6，用以計算  $c = X \cdot v \bmod r$ 。在步驟 S 6 用以判定該值是否成為 0，若  $c = 0$  則在步驟 S 7 用以計算  $d = (f + c \cdot K_s) / u \bmod r$ ，並在步驟 S 8 用以判定 d 是否為 0，若  $d \neq 0$ ，則在步驟 S 9 將 c 及 d 作為電子簽名資料進行輸出。如果，將  $x$  設定為 160 位元長之長度，則電子簽名資料將形成 320 位元長。

在步驟 S 6 中，使  $c = 0$  時，則返回到步驟 S 3 用以生成並修正新的亂數。同樣，在步驟 S 8 後  $d = 0$  時，也返回到步驟 S 3 用以生成並修正系數。

(3-3) 離散公開編號方式之電子簽名的驗証

其次，將使用公開編號規範方式之電子簽名的驗証方法，使用圖 1.2 加以說明。在步驟 S 1.1，將以做為信息  $\cdot p$  為標數， $a, b$  為椭圓曲線之係數 (椭圓曲線： $y^2 = x^3 + ax + b$ )，將 G 為椭圓曲線上之基點， $t$  為 G 之位數， $G$  及  $K_s \times G$  公開編號 ( $0 < K_s < t$ )，在步驟 S 1.2 使電子簽名資料 c 及 d 用以驗證後若滿足  $0 < c < t$ ， $0 < d < r$ ，將此滿足時，則在步驟 S 1.3，用以計

五、發明說明 (91)

被宣改，但可如用以保持對應於公開編號之密鑰編號來用以生成電子簽名。

(3-4) 由共同編號規範方式之相互認証

其次，將使用共同編號規範方式之相互認証方法，使用圖 1.3 加以說明。在圖 1.3 中，做為共同編號規範方式使用有 DES，但如前述有同樣之共同編號規範方式則皆可。圖 1.3 中，首先，使 B 用以生成 6 位元之亂數 R\_d，並將 R\_d 及自己之 ID (b) 發送至 A，將此接收後，B 用以生成新的 6 位元之亂數 R\_a，並以 R\_a, R\_b, ID (b) 之順序，以 D E S 之 C B C 模式使用編號 K\_a b 用以暗號化資料，並遞送至 B，若依據圖上所示 D E S 之 C B C 模式處理傳輸，則相對於 R\_a 為 M\_1, R\_b 為 M\_2, ID (b) 為 M\_3，而初期值：I\_V = 0 時便收到 I\_1, E\_2, E\_3 作為暗號。

將此接收後之 B，係將接收資料以編號 K\_a b 進行譯碼化，接收資料之譯碼化方法，係首先，將暗號文 E\_3 以編號 K\_a b 進行譯碼化，取得亂數 R\_a，其次，暗號文 E\_2 以編號 K\_a b 進行譯碼化，並與該結果將 E\_1 進行對應性邏輯和，取得 R\_b，最後，確認文 E\_3 以編號 K\_a b 進行譯碼化，差異結果將 E\_2 進行對應性邏輯和，取得 ID (b)。如此若取得之 R\_a, R\_b, ID (b) 之內，使 R\_b 及 ID (b)，用以驗証 B 是否與發送的進行一致，通過驗証時，則 B 係將 A 做為正常並加以認証。

A7

B7

## 五、發明說明 (92)

接者 B，係在認証後用以生成 (生成方法，係使用亂數) 之對該時間範圍 (Session Key) 以下，做為  $K_{es}$  )。而且，以  $R_b$ 、 $R_a$ 、 $K_{es}$ 之順序，以 D-E S 之 C-B-C 次序使用論述  $K_{ab}$  並進行量化，並送途到 A。

再此接收後之 A，係若將收資料以論述  $K_{ab}$  進行譯碼化，涉收資料之詳碼化方法，係依 A 之譯碼處理而得，所以在接收時即說明，如此無須將之  $R_a$ 、 $R_b$ 、 $K_{es}$  之內，使  $R_b$  及  $R_a$ ，用以驗證 A 是否與前述的進行一致，通過驗證時，則 A 係將 B 做為正確並加以認證，在相互互用以確認對方之後，對括時間範圍  $K_{es}$ ，係被利用做為認證後之認證及應用的共同鑑識。

尚有，在接收資料之驗證時，找到不正確，不一致時，則無為相互認證及失敗而以中斷處理。

## (3-5) 公開驗此證明書

其次，對於公開驗此證明書使用圖 1-4 加以說明，公開驗此證明書，係公開驗此證明方式之認證局 (CA : Certificate Authority) 進行發行的証明書，使用者將自己之 ID，公開驗此證明書等資料向認證局提出，認證局側用以解加認證局之 ID 或有效期限等資訊，並由根據認證局而以附加署名方式作成之認證書。

圖 1-4 所示為認證此證明書，係含四項證明之方案號碼，認證局對證明書利用者分派的證明書選項，使用於電子簽名之真偽及參數，認證局之名稱，證明書之有效期間。

本辦法人適用於中國標準委員會(CNS11444)規格(220+297公釐) - 95 -

A7

B7

## 五、發明說明 (94)

圖由結合驗號的相互認証方略，使用圖 1-5 加以說明。圖 1-5 中，係用公開驗此證明方式係使用 ECCC，假如前述若以認證之公開驗此證明方式則可，又，鑑匙大小也非 16 位元不可，並 15 位，首先使 B，用以生成 6 4 位元，並發送到 A，將此接收後之 A，係帶以生成的前 9 4 位元之亂數  $R_b$  及模數  $p$  與之的亂數  $A_k$ 。而且，將基底 G 乘出進行  $A_k$  後之  $A^y = A_k \times G$ ，對  $R_a$ 、 $R_b$ 、 $A_y$ 、 $V$  (X座標及 Y座標) 用以生成電子簽名  $A$ 、 $Sig$ ，並與 A 之公開驗此證明書一起送達至 B，於此  $R_a$  及  $R_b$  分別有 6 4 位元， $A$  之 X 座標及 Y座標分別有 1 6 0 位元，所以對合計 4 4 8 位元用以生成電子簽名。電子簽名之生成方法係在圖 1-2 已作說明，所以省略其詳細說明。又，公開驗此證明書也在圖 1-4 已做說明，所以也省略其詳細說明。

接收 A 之公開驗此證明書， $R_a$ 、 $R_b$ 、 $A_y$ ，電子簽名  $A$ 、 $Sig$  後之 B，係使 A 送來之  $R_b$ ，用以驗證是否與 B 生成的一致，其結果，送來一致時，則將 A 之公開驗此證明書內的電子簽名以認證之公開驗此證明書並取出 A 之公開驗此。對於公開驗此證明書之驗證，係使用圖 1-4 已做說明，所以省略其說明。而且，使用取出後之 A 的公開驗此證明書名  $A$ 、 $Sig$ ，電子簽名之驗證方法係已在圖 1-2 做了說明，所以省略其說明。在電子簽名之驗證進行成功之後，B 係將 A 做為正確並加以認證。

本辦法人適用於中國標準委員會(CNS11444)規格(220+297公釐) - 97 -

A7

B7

## 五、發明說明 (95)

證明書利用者之名稱 (利用者 ID)，認證書利用者之公鑑號及電子簽名。

電子簽名，係對證明書之來路署名，認證局對證明書利用者分派的證明書選項，使用於電子簽名之算法及參數，認證局之名稱，證明書之有效期限，證明書利用者之名稱及認證書利用者之公開驗此證明書選項並用以生成亂數碼，對該亂數後係使用認證局之密鑑匙生成之後之密鑑，該電子簽名之生成，係會如被適用圖 1-1 說明的處理流程。

認證局，係進行發行圖 1-4 所示公開驗此證明書，同時更新有效期限碼及之公開驗此證明書，為了進行斯以選擇不正當行為之利用者作成不正確者名單，進行管理，配布 (將此前稱為取消：Revocation)。又，根據必要也進行公開驗此證明書，藉證明書之生成。

另外，在利用該公開驗此證明書時，利用者係使用自己保持之認證局之公開驗此證明書，用以驗證該公開驗此證明書電子簽名，在電子簽名之驗證進行成功之後由公開驗此證明書取出公開驗此，並利用該公開驗此。因此，利用公開驗此證明書之所有利用者，係有必要保持共同之認證局之公開驗此，尚有，對於電子簽名之驗證方法，係在圖 1-2 已做說明所以省略其詳細說明。

## (3-6) 由公開驗此證明方式之相互認証

其次，將使用公開驗此證明方式之 1-6 0 位元長之密鑑。

A7

B7

## 五、發明說明 (96)

其次，B 係用以生成比模數  $p$  小之的亂數  $B_{k-1}$  而且，將基底 G 乘出進行  $B_{k-1}$  之點  $B = B_{k-1} \times G$ ，對  $R_b$ 、 $R_a$ 、 $B$ 、 $V$  (X座標及 Y座標) 用以生成電子簽名  $B$ 、 $Sig$ ，並與 B 之公開驗此證明書一起送達至 A。

接收 B 之公開驗此證明書， $R_b$ 、 $R_a$ 、 $A_y$ ，電子簽名  $B$ 、 $Sig$  後之 A，係使 B 送來之  $R_b$ ，用以驗證是否與 A 生成的一致，其結果，送來一致時，則將 B 之公開驗此證明書內的電子簽名以認證局之公開驗此證明書並取出 B 之公開驗此，而且，使用取出後之 B 的公開驗此證明書名  $B$ 、 $Sig$ ，在電子簽名之驗證進行成功後，A 係將 B 做為正確者並加以認證。

使兩者在認證進行成功時，則 B 係用以計算  $B \times X$   $A_y$  (B 係係數，但  $A_y$  係因為在椭圓曲線上之點，所以必要將座標上之點的橫座標計算)，而 A 係用以計算  $A \times B \times V$ ，並判斷等號之 X座標的下位 6 4 位元作為對話時間驗先並使用於以後之進訊 (將公開驗此證明書為 6 4 位元係數之與認證局驗證時)。當然，由於進訊用以生成對話時間驗先也非，非下位 6 4 位元也可，尚有，藉互認後之密鑑選訊中，發送資料係不僅以對話時間驗先並暗號化，而首則有電子簽名。

在電子簽名之驗證或接收資料之驗證時，發現不正確，不一致時，則為相互認証進行失敗並用以中斷處理。

## (3-7) 使用椭圓曲線驗證之驗證方法

本辦法人適用於中國標準委員會(CNS11444)規格(220+297公釐) - 98 -



A7  
B7

## 五、發明說明 (100)

**Idmem**：記錄裝置識別資訊，記錄裝置固有之識別資訊。

**Kake**：認証產生器，記錄再生器 300 使用於相互認證時之認証裝置。

**lvmem**：新測值，相互認證或認證等級被使用於相應或現之初期值。

**Kstr**：保存地址，匯存資訊論述其存儲區系資訊之址址地。

**Kr**：亂數生成論述。

**S**：權

將此之資料各自保持於個別之區段，外部記錄裝置 402 係用以保持數字（以本例爲四個）之存儲信息資料，分別以圖 4 與圖 5 已說明之資料，譬如保持於圖 2.6，或圖 2.7。對於圖 2.6，圖 2.7 之構成的差異僅在後者加以說明。

(6) 記錄再生器，記錄裝置間之相互認證過程

(6-1) 相互認證處理之概要

圖 2.0 係所記錄再生器 300 及記錄裝置 400 之認證順序流程圖，在步驟 S 4.1 中，使利用者將記錄裝置 400 插入到記錄再生器 300，以非接觸方式可通過記錄裝置時，而不必進行插入。

在記錄再生器 300 上以設定記錄裝置 400，則從

A7  
B7

## 五、發明說明 (101)

圖 3 所示記錄再生器 300 內之記錄裝置檢測與處理（未顯示），將記錄裝置 400 之裝置並行運行如到控制部 3.0.1。其次，在步驟 S 4.2 中，記錄再生器 300 之控制部 3.0.1，係通過記錄裝置識別器 3.0.3 用以發送初期化指令到記錄裝置 400.0. 將此前後之記錄裝置 400，係在記錄裝置識別器 4.0.1 之控制部 4.0.3，通過通訊器 4.0.4 用以接收指令，並使記錄裝置若被設定則進行消除，即設定於未認證狀態。

其次，步驟 5.4.4 中，記錄再生器 300 之控制部 3.0.1，係用記錄裝置 400 之記錄裝置識別器處理部 4.0.1 用以指定論述該裝置，向右，有關該裝置資訊之詳情將後述。步驟 5.4.5 中，記錄再生器 300 之控制部 3.0.1，係從上述記錄裝置到記錄裝置 4.0.0 之內部記憶體 4.0.5 被指派的論述之後之記錄裝置識別資訊 Idmem。在步驟 S 4.6 中，記錄再生器 300 之控制部 3.0.1，係使該記錄裝置識別資訊 Idmem 到記錄再生器識別處理部 3.0.2，並根據記錄裝置識別資訊 Idmem 使認證論述 Kake 生成，做為認證論述 Kake 之生成方法，詳載如如下進行生

## 【附 3】

KakeDES(Mkakc, Idmem^lvake)

據此，Mkakc，係在記錄再生器 300 及記錄裝置 400 (參考圖 3) 之間在被執行相互通認或標識時用以生成必要的認證論述 Kake 之記錄裝置認證用主論述，此第

A7  
B7

## 五、發明說明 (102)

如前所述關於記錄再生器 300 之內部記錄裝置 3.0.7 又，**Idmem**，係在記錄裝置 400 內有之記錄裝置識別資訊，並非 lvake，係記錄裝置識別初期值，又，在上述式中，D E S ( )，係將第一引數設為時間辨起，將第 2 引數設為以 D E S 進行標準化的因數，將第 3 依循 6.4 元素單位之非線性邏輯。

譬如適用圖 7、圖 8 所示 D E S 構成時，則將該顯示於圖 7、8 之信息 M 作為記錄裝置識別資訊：Idmem，並所識別起 K 1 為裝置识别字頭為：Mkakc，將初期值 I V 作為 lvake 以便取得之輸出形式稱為識別匙 Kake。

其次，在步驟 S 4.7 進行相互認證及對話時間辨期 Kake 之生成處理，相互通認，係在記錄再生器各論述處理部 3.0.2 之論述／淨化部 3.0.8 及記錄裝置各論述處理部 4.0.1 之論述／淨化部 4.0.2 之間進行，將其仲介使記錄再生器 300 之控制部 3.0.1 進行。

相互認證處理，係譬如依據前述圖 1.3 所說明之處理可執行，圖 1.3 所示構成中，A、B 係分別對應於記錄再生器 300 及記錄裝置 400。首先，將記錄再生器 300 之記錄裝置識別處理部 3.0.2 用以生成亂數 R b，並生成亂數 R b 及自己之 D 之記錄再生器識別資訊 IDdev 之後到記錄裝置 400 之記錄再生器識別處理部 4.0.1，由於，記錄再生器識別資訊 Iddev，係將記錄裝置被構成在記錄再生器 300 內之記錄裝置的再生器固有之亂數子。在記錄再生器識別處理部 3.0.2 之內部記錄中用以記錄記錄再

A7  
B7

## 五、發明說明 (103)

生器識別資訊 IDdev 做為構成也可。

接收亂數 R b 及記錄再生器識別資訊 IDdev 後之記錄裝置 4.0.0 之記錄裝置識別資訊處理部 4.0.1，係用以生成新的 6 位元之亂數 R a，即 R a，R b，及記錄再生器識別資訊 IDdev 之順序，以 D E S 之 C B C 模式用以認證論述 Kake 進行標準化，並發送到記錄再生器 300 之記錄裝置識別處理部 3.0.2。譬如，當接收到 7 所示 D E S 之 C B C 模式處理情況，則相當於 R a 為 M 1，R b 為 M 2，IDdev 為 M 3，而使初期值為：I V=lvmem 之輸出 E 1，E 2，E 3 之串接號碼。

接收論述文 E 1、E 2、E 3 後之記錄再生器 300 之記錄裝置識別資訊處理部 3.0.2，係將所接收資料以認證論述 Kake 進行標準化，接收資料之詳述方法，首先，將論述文 E 1 以認證論述 Kake 進行辨識，將其結果與 E 1 之記錄裝置識別，並取亂數 R a。其次，將論述文 E 2 以認證論述 Kake 進行標準化，將其結果與 E 2 進行辨析性邏輯，並取亂數 R a。最後，將論述文 E 3 以認證論述 Kake 進行標準化，將其結果與 E 3 進行辨析性邏輯，並取亂數 R a。如此被取得之 R a，R b，記錄再生器識別資訊 IDdev 之內，使 R b 及記錄再生器識別資訊 IDdev，用以認證記錄再生器 300 發送的是否一齊，通過訊息辨認時，記錄再生器 300 之記錄再生器識別處理部 3.0.2 係將記錄裝置 4.0.0 依其工作參數並加以認證。

AF  
BY五、發明說明<sup>(104)</sup>

其次，記錄再生器 3 0 0 0 之記錄再生器號碼處理部 3 0 2，係在認證後用以生成（生成方法，係使用亂數）使用之對話時間鑑匙（Session Key（以下簡稱為 Kies），而且，依 R b 、 R a 、 Kies 之順序，由 D E S C C B 模式使用輪匙 Kake，初期將 ivmem 進行詳情化，並送達識錄裝置 4 0 0 之記錄裝置處理部 4 0 1。

若此接收後之記錄裝置 4 0 0 之記錄再生器號碼處理部 4 0 1，係將接收資料以輪匙 Kake 進行詳情化，接收資料之詳情化方法，係與記錄再生器 3 0 0 0 之記錄再生器號碼裝置部 3 0 2 中之詳情化處理同樣，所以在此省略說明，如此即表示之 R b 、 R a 、 Kies 之內，依 R b 及 R a ，用以檢驗所記錄裝置 4 0 0 設置的是否一致，通過該輪匙時，記錄裝置 4 0 0 之記錄再生器號碼處理部 4 0 1 係將記錄再生器 3 0 0 0 併存並加以認定，在相互認證對方之後，則對話時間鑑匙 Kies。係為了認證後之秘密資訊作為共同鍵被利用。

尚有，在接收資料之輪匙時，後述不正當，不一致時，則要相互認證作為失敗並用以中斷處理。

在相互認證成功時，由步驟 S 4 6 遷到步驟 S 4 9，將對話時間鑑匙 Kies 以記錄再生器 3 0 0 0 之記錄再生器號碼從 3 0 2 加以保持，同時關係於相互認證時並用以決定認證終了標記。又，在相互認證失敗時，則跳到步驟 S 5 0，以認證處理過程用以檢驗再生器之後之對話時間鑑匙 Kies，同時用以檢驗背後修了標記，向有已經被消除的

AF  
BY五、發明說明<sup>(105)</sup>

不一定必要請參照處理。

尚有，使記錄裝置 4 0 0 由記錄裝置插入點被取出時，則從記錄再生器 3 0 0 0 內之記錄裝置檢測裝置，將記錄裝置 4 0 0 並取出之事項通知到記錄再生器 3 0 0 之監視部 3 0 1，將此接收後之記錄再生器 3 0 0 之控制部 3 0 1，係對記錄再生器 3 0 0 之記錄再生器號碼處理部 3 0 2 對應於記錄裝置插入點而將此之認證終了標記進行標記命令，將此接收後之記錄再生器 3 0 0 之記錄再生器號碼處理部 3 0 2，係對應於記錄裝置插入點而將此之認證終了標記進行清潔命令。

尚有，於此係對於將相互認證或處理根據圖 1 3 所示程序進行執行之列舉了說明，但不限定於上述之認證處理例，譬如用以執行根據圖 1 3 所示之認證或處理也可。

又，圖 1 5 所示手續中，將圖 1 3 之 A 當作記錄再生器 3 0 0 ，將 B 當作記錄裝置 4 0 0 ，而 B 當作記錄裝置 4 0 0 第一級次段 A：記錄再生器 3 0 0 之 D 當作記錄裝置區中之輪匙區段中的記錄裝置檢測資訊並進行相互認證處理也可。本發明中若執行之認證處理手續，係可選用兩種之認證，並非限定於上述之認證處理。

## (6-2) 相互認證時之輪匙區段的轉換

本發明之黃片處理裝置中之相互認證處理的 1 個特徵，係在記錄裝置 4 0 0 0 用以構成複數之輪匙區段（ex. N 次之輪匙區段），並使記錄再生器 3 0 0 用以推

AF  
BY五、發明說明<sup>(107)</sup>

記錄再生器之記錄裝置，圖 3 之中內部記錄裝置 3 0 7，或記錄再生器 3 0 0 之具有其他的記錄元件，在認證處理時藉由圖 3 之控制部 3 0 1 存取現並進行依欲設立資訊後之輪匙區段指定位。

記錄再生器 3 0 0 之中內部記錄裝置 3 0 7 的記錄裝置認證用主輪匙 Mkey，係根據分別之指定輪匙區段的設定被設定後之記錄裝置用主輪匙，形成僅可對於指定輪匙區段，形構成該用主輪匙區段以外之輪匙區段的相互認證不成立。

由於 1 9 處理流程，在記錄裝置 4 0 0 之內部記錄裝置 4 0 5 係被設定有 1 ~ N 之 N 個輪匙區段，在各輪匙區段容納有記錄裝置識別資訊，認證輪匙，前項值，認證點，輪匙數生成輪匙，據，至少便從互用之輪匙資料在各區段做為不同資訊被存。

如此，記錄裝置 4 0 0 之輪匙區段的輪匙資料構成，係在各區段不同。因此，譬如，使某記錄再生器 A 使用並容納於內部記錄裝置之記錄裝置識別資訊 Mkey 可進行認證處理之輪匙區段係區段區段 No. 1，又使另外規格之記錄再生器 B 可認證之輪匙區段係區段另外部之輪匙區段，譬如形或可設定成識別碼區段 No. 2。

在後段會更詳細加以說明，但尚須留意容納於記錄裝置 4 0 0 之中並記憶部 4 0 2 時，因未被存容納於各輪匙區段後之保存輪匙 Ktr 被隱號化處理，並形成被存容納，更具體而言，係將存儲信息區段進行標號化並存儲信息區

AF  
BY五、發明說明<sup>(106)</sup>

定（圖 2 之認證流程中之步驟 S 4 4 ） 1 個之輪匙區段用以執行認證處理之點。如檢查圖 1 9 所示之說明，在該構成或記錄裝置 4 0 0 0 之輪匙區段部 4 0 1 的內部記錄裝置 4 0 5 被形成有複數之輪匙區段，便分別用以容納不同的輪匙資料，I D 資訊等各類資訊，在第 2 0 步接續之記錄再生器 3 0 0 及記錄裝置 4 0 0 時被執行之相互認證處理，係對圖 1 9 之記錄裝置 4 0 0 的複數輪匙區段之 1 個輪匙區段執行。

先前，用以執行記錄裝置及其再生器資料之相互認證處理的構成，係使用於相互認證之輪匙：從記錄裝置 1 係依技術共同的論點，因此，當各製品發送對象（業者），或各製品消費更認證輪匙，是在記錄再生器，及記錄裝置之認證處理成為必要之輪匙資料在雙方之機器中成為必要進行更，因此當知在被存於新的被存後之記錄再生器的記錄處理成為必要之輪匙資料，係不對應於新在先被存實之記錄裝置的認證處理成為必要之輪匙資料，新的記錄再生器，係將單式的記錄裝置會形成為不能存取之事態。相反地在新的單式的記錄裝置及舊的單式的記錄再生器的關係也會發生同樣之事態。

本發明之實利處理係實，係如圖 1 9 所示首先在記錄裝置 4 0 0 0 做用複數不同輪匙組被存容納有識別區段，記錄再生器係存於各製品發送對象（業者），或在各製品，機器，型式，應用程式，被設有屬屬於於認證處理之輪匙區段，而被設有指定輪匙區段，該被定資訊，係被導納於

AF  
BY五、發明說明<sup>(107)</sup>

記錄再生器之記錄裝置，圖 3 之中內部記錄裝置 3 0 7，或記錄再生器 3 0 0 之具有其他的記錄元件，在認證處理時藉由圖 3 之控制部 3 0 1 存取現並進行依欲設立資訊後之輪匙區段指定位。

記錄再生器 3 0 0 之中內部記錄裝置 3 0 7 的記錄裝置認證用主輪匙 Mkey，係根據分別之指定輪匙區段的設定被設定後之記錄裝置用主輪匙，形成僅可對於指定輪匙區段，形構成該用主輪匙區段以外之輪匙區段的相互認證不成立。

由於 1 9 處理流程，在記錄裝置 4 0 0 之內部記錄裝置 4 0 5 係被設定有 1 ~ N 之 N 個輪匙區段，在各輪匙區段容納有記錄裝置識別資訊，認證輪匙，前項值，認證點，輪匙數生成輪匙，據，至少便從互用之輪匙資料在各區段做為不同資訊被存。

如此，記錄裝置 4 0 0 之輪匙區段的輪匙資料構成，係在各區段不同。因此，譬如，使某記錄再生器 A 使用並容納於內部記錄裝置識別資訊 Mkey 可進行認證處理之輪匙區段係區段區段 No. 1，又使另外規格之記錄再生器 B 可認證之輪匙區段係區段另外部之輪匙區段，譬如形或可設定成識別碼區段 No. 2。

在後段會更詳細加以說明，但尚須留意容納於記錄裝置 4 0 0 之中並記憶部 4 0 2 時，因未被存容納於各輪匙區段後之保存輪匙 Ktr 被隱號化處理，並形成被存容納，更具體而言，係將存儲信息區段進行標號化並存儲信息區

五、發明說明（<sup>108</sup>）

段以反存輪匙進行強制化處理。

如果圖 1-9 所示保存輪匙，係在各級設置或僅為不同級別。因此，能以指定不同輪匙區段在該級別之 2 個不同設定的記錄再生輪匙，係將被認可於某子級之記錄再生器的記錄體之存儲信息防止以前者共同利用，即，形成不同級別之記錄再生器。係符合於分別之設定也可利用被容納於記錄體之後的存儲惟權。

另一方面，對於各輪匙級別可共同化資料係也可進行共同化，譬如將認證用之記錄資料，保存輪匙資料構成不同級別也可。

如此在記錄裝置便由被啟之不同的輪匙資料用以構成輪匙級別作為資料，譬如如可別以記錄再生器 300 之機種別（安慶型、瀋陽型等）將各自輪匙級別設定成不同，或在各自應用式將各自輪匙級別設定成不同。譬如對於在日本販賣者係亞洲地區輪匙級別為 N o . 1，在美國販賣之記錄再生器係將各自輪匙級別為 N o . 2，故在各地區也可構成進行不同的輪匙級別設定。以如此之構成，在分別不同販賣地點使用，而在記錄裝置以不同策略應對被容納之存儲信息，並假使如記錄卡被記錄後經由承運商轉送至日本，或由日本轉送至英國，即以被形成不同級別設定之記錄再生器不能使用，所以可防止容納於記錄體之存儲信息的不正確，無秩序之流逝。具體而言，係以不同保存被啟 Ksix 來被強制化之存儲惟權，啟動被啟 Kcon 在 2 級間可排除互相利用的狀態。

本技術是適用中國國家標準（CNSIA）規格（JB/T 297 公司） - 111 -

五、發明說明（<sup>109</sup>）

進而，圖 1-9 所示記錄裝置 400 之內部記錄體

405 的輪匙區段 1 ~ N 段之至少 1 個輪匙區段，譬如將 N o . N 之輪匙區段在其中之一的記錄再生器 300 也可被構成共同利用之輪匙區段也可。

譬如，在全部之機器用輪匙區段 N o . N 用以容納可認證的記錄裝置認證用主輪匙 Mlike，在記錄再生器 300 之機種別，各應用型別，各設備範圍等以無關係地為可流通之存儲信息可處理。譬如，以各別的輪匙區段 N o . N 之保存輪匙被容納於記錄卡之暗號化存儲信息，譬如在全部之機器中形成可利用的存儲信息。譬如將資料資料等以共同可利用之輪匙區段的保存輪匙進行強制化之記錄裝置，將記錄卡，譬如同樣用以容納共同之記錄裝置認證用主輪匙 Mlike 在機器之間之存儲再生機器等進行統一，由記錄卡可由資料之譜寫可再生處理。

圖 2-1 係顯示本發明之資料處理裝置中共有被數之輪匙級別的記錄裝置利用者，記錄再生器 210 係為日本之製品的記錄再生器，在兩記錄裝置之輪匙區段 N o . 1 ~ 4 之間持有主輪匙並成立認證惟權。記錄再生器 210 係對 U S 之製品的記錄再生器，在兩記錄裝置之輪匙區段 N o . 2 ~ 4 之間持有主輪匙並成立認證惟權。記錄再生器 210 係對 E U 之製品的記錄再生器，在兩記錄裝置之輪匙區段 N o . 3 ~ 4 之間持有主輪匙並成立認證惟權。

譬如記錄再生器 210 係，係與記錄裝置 A、210 4 之輪匙區段 1 與輪匙區段 4 之間便能認證成立，並

本技術是適用中國國家標準（CNSIA）規格（JB/T 297 公司） - 112 -

五、發明說明（<sup>110</sup>）

分別便實施理清處理後之存儲信息通過被容納於輪匙級別的保存輪匙並被容納於外部記錄體。記錄再生器 210 2，係與記錄裝置 B、210 5 之輪匙區段 2 或輪匙區段 4 之間便能認證成立，並分別便實施理清處理後之存儲信息通過被容納於輪匙級別的保存輪匙並被容納於記錄體。記錄再生器 210 3，係與記錄裝置 C、210 6 之輪匙區段 3 或輪匙區段 4 之間便能認證成立，並分別便實施理清處理後之存儲信息通過被容納於輪匙級別的保存輪匙並被容納於外部記錄體。對於，將記錄裝置 A、210 4 裝著於記錄再生器 210 2，或記錄再生器 210 5 之輪匙區段 1 之保存輪匙被認證處理後之存儲信息，係在記錄再生器 210 2，記錄再生器 210 3 及輪匙區段 1 之間便能認證不成立或以為不可利用。另外，以輪匙級別 4 之保存輪匙被認證處理後之存儲信息，係在記錄再生器 210 2，記錄再生器 210 3 及輪匙級別 4 之間便能認證成立所以成為可利用。

如上述，本發明之資料處理裝置中，在記錄裝置由被啟之不同輪匙並能用以構成輪匙級別，另外，在記錄再生器，係將特定之輪匙級別用以容納可認證之主輪匙並為擴張，所以根據擴張的利用惟權可用以設定存儲信息之利用限制。

而前，1 項之記錄再生機器中將有指定之輪匙級別數為被啟數，譬如假使 1 ~ k，其他之記錄再生器中將可指定之輪匙級別也可能被啟數 p ~ q，又，將可共同利用之

五、發明說明（<sup>111</sup>）

輪匙級別被構成被啟數也可。

（7）由記錄再生器對記錄裝置之下載處理

其次，本發明之資料處理裝置中，對於由記錄再生器 300 在記錄裝置 400 之外部記錄體用以下載存輪匙信息之處理加以說明。

圖 2-2 係用以說明由記錄再生器 300 對記錄裝置 400 用以下載存輪匙信息之序流演繹。尚可圖 2-2 中，係作為在記錄再生器 300 及記錄裝置 400 之間已經完成上述之相互認證處理。

步驟 S 5-1 中，記錄再生器 300 之控制部 301，係使用讀取部 304 由用以容納存儲惟權後之深層 500 課用以存儲固定之格式之資料，或使用資訊部 305 由資訊庫 600 依據既定之模式用以接收資料。而且，記錄再生器 300 之控制部 301，係將資料內之Header（Header）部分（參考圖 4-1）發送至記錄再生器 300 之記錄再生器識別部 302。

其次，步驟 S 5-2 中，在步驟 S 5-1 用以接收當（Header）之後之記錄再生器識別部 302 的控制部，係在記錄再生器識別部 302 之暗號化／譜寫化部 308 便根據 A 計算，核對惟 A，係如圖 2-3 所示，將被保存於記錄再生器識別部 302 之內部記錄體 307 的核對惟 A 生成惟權 Kicva 係為識別，將識別資訊（Content ID）及處理方針（Usage Policy）並將信息依據圖 7 之說明

A7

B7

## 五、發明說明(112)

之  $I - C V$  計算方法被計算，尚有初期值，係作為  $I = V = 0$ ，但在記錄再生器號碼處第 302 之內部記憶體 307 用以備核對該 A 生成用初期值  $I = V = 0$  放置，將此加以使用也可。最後，用以比較核對該 A 及被容納於累加（Header）內之核對值： $I - C V a$ ，在進行一致時則得到步驟 S 5.3。

首先如圖 7-4 便說明之換對價 A、I I C v a，係為了用以統識別實體、處理方針之簽收的核對證。將被保存於記錄再生監控範疇表單 3-02 之內部記憶體 30-7 的核對價 A 生成轉換 Kicva 為誰為誰，將審覈別資訊 (Content ID) 及處理方針 (Usage Policy) 與哪個依循並已說明之 I C V 由其實質計算核對準，由與被容納於集管 (Header) 之核對標記 : I C V a 進行一致後時，附則判斷別資訊，處理方針無異狀。

其次，步驟 S 5 3 中，記錄再生器導號感應部 3 0 2 之控制部 3 0 6，係使配送輪點 Kd1 之生成在記錄再生器導號感應部 3 0 2 之導號／譯碼化部 3 0 8 進行。參為配送輪點 Kd1 之生成方法，係僅如進行如下所述。

[ 84 ]

$Kdis = DES(MKdis + Content \parallel D^*)Vdis$

於此，MKdis，係為了用以生成配送匙匙 Kdis 之配送匙匙用主匙匙。此係，如前述客容納於記錄再生器 300 之內部記憶體的鍵匙，又 Content ID 係存儲信息資料之惟一能部的識別資訊。進而 IVdis，乃配送匙匙用初頭碼。又，

本教材尺寸為寬 210 × 高 297 公釐 (CN564) - 115 -

A7  
B7

### 五、骨髓瘤 (<sup>134</sup>I)

其次記載再生細胞層處第 3-0-2 之標示部 3-0-6，係在記錄再生細胞層處或標示 3-0-2 之所指，詳圖化部 3-0-8 稱核對標 B (I C V b) 計算。核對標 B，係如圖 2 所示，將標示部 3-0-2 在記載再生細胞層處第 3-0-2 之內部記號 3-0-7 的核對標 B 生成論述 Kieb 做為論述，詳附才計算之後即得之細胞層和值以 D E S 進行論述化並加以生成。最後，用以比擬核對標 B 及 Header 內之 I C V b，在進行一致後即得步驟 5-57。

如前面圖 4-1 中已做了說明，被列僅 B、I C V b，係用了以被列區段資訊儲備 Kbit，存儲信息總量 Kcon，甚者資訊（B IT）之累加的總對值。所被保存於記再生號或裡部 3 0 2 之內即記備存 3 0 7 的核對數 B 生級編號 Kiczbv 係為數字，甚於區段資訊儲備 Kbit，存儲信息總量 Kcon 及甚區段資訊（B IT）分別成 8 倍單位並進行逐級性產生和將取用後以 D E S 進行唯化後成為之後級對值 B，與被容納到標頭（Header）內之核對值：

步驟 S 5 7 中，記錄再生器總體處理部 3 0 2 之抑制部 3 0 6。係在記錄再生器總體處理部 3 0 2 之抑制／譯碼化部 3 0 8 使中間檢對值計算。中間檢對值，係如圖 2 5 所示，將被保存於記錄再生器總體處理部 3 0 2 之內部記憶體 3 0 7 的總校對值生成論理 Kiev 依此編號，並將

—  
—  
—

A7  
B7

## 五、發明說明(113)

上述式中，DES（）。係將第 1 引數做為暗號輸匙，而以暗號化第 2 引數之值的函數。演算一係顯示 64 位單元之操作性邏輯和。

步驟 5 54 中，記錄再生器帶號或處理部 3 02 之控制第 3 06，係用以記錄再生器帶號或處理部 3 02 之帶號／速率或處理部 3 08，在步驟 5 55 之使用後之記錄或 Kdls，適應選擇部 3 04 帶收後之速率 500，或進行速遞或處理部 3 05 由脈訊帶號 6 00 作答音於接收後之資料的量並將之置於資料庫編輯處 Kbit 及存儲器中地點 Kcon（步驟 5 56）之選擇處或處理處。如被繼不計算第 4 此步驟其資料庫編輯處 Kbit 及存儲器地點 Kcon，係在 D V D 、 C D 等之選擇，或脈訊地點等之速遞路面上，藉由記錄或處理部 Kdls，將先被實質地脈訊化。

追步，步頻 555 中，起點再生器帶寬處理部 302 之接頭部 306，係用機械再生器帶寬處理部 302 之接頭號／源極化部 308，在步頻 S 554 中以源極化部 308，以源極化部 308 與源極化部 306 之區隔資訊碼 Kbit 用以源極化部資訊（B IT）而被應用於步頻 4 此等資訊碼（B IT）係在 D V D 、 C D 等之媒體，或視聽路等之憑藉階上，藉由前述之 Kbit 將先被實際應用於此處。

進而，步驟 S 5 6 中，記錄再生器號或選項 3 0 2 之控制部 3 0 6，係將基段資訊總匙 Kbit，存儲信息流匙 Kcos 及底層資訊 (B I T) 分割成 8 組元單位，將此等全部進行操作性累加和（加算，減算等），其中之一運算即可

本版块文章请用中文简体字（CNS简体字集或 210×207 字集）

A7  
B7

五、發明說明(115)

保持放著全部之存儲信息核對做為信息依據圖 7 說明之 I C V 計算方法進行計算。尚有，做為初期值  $I V = 0$ ，但在記錄再生器確定此運算 3.0.2 之內部記憶體 3.0.7 用以保證總計對生成值用初期值  $I V = 0$  設定。將此進行便用也可。又，生成後之時間核對值，根據其必要性於記錄再生器 3.0.0 之記錄再生器置置時，日期為 3.0.2 故為。

該中間板對值，係將板對值A、板對值B、全形之存儲與級數對板為各項信息會生成，將對於形成各項板對之驗證對象的資料之驗證藉由中間板對值之板對為處理而生性可。可是，本實驗則中，係將板為系統總體而具有共同的非級數之驗證處理。及在下載處理後僅僅各記錄再生器300張為佔有之占有資料為進行了獨創性而別於級數對板為系統為可執行，由中間板對值與板對視頻之不同板對值，即板板對值！CVT。及記錄再生器有板對值ICVdet，分別根據中間板對值能為可生成。對於此等板對値俱在分別加以說明。

記錄再生器號或處理部 302 之控制部 306，依在記錄再生器號或處理部 302 之總序／總步驟部 308 依循其總序或步驟之次序，將該步驟之總序或步驟編號指派於 I C V T 之計算。總序指派於 I C V T 之起始如圖 5 所示，萬能保存的記錄再生器號或處理部 302 之內部記憶體 307 的系統名稱為 Keys 依循為縮寫，將中間空間以 D E S 行單字並加生成後，所以比以前生成後之總序指派於 I C V T 及在步驟 551 進行保存故有的。

Journal of Health Politics, Policy and Law, Vol. 32, No. 4, December 2007  
DOI 10.1215/03616878-32-4 © 2007 by The University of Chicago

## 五、發明說明 (116)

是資料之記錄再生處理在系統集合全體中共同之署名論述。

如前圖四中已做了說明，總級對值 I C V t，係為了用以 I C V a、I C V b，各存儲信息區段之核對值全部之次數之總對值。因此，藉由上述之處置使被生成之後級對值與被帶至於首管 (Header) 內之核對值：

I C V t 在進行一些後辦，則第判斷 I C V a、I C V b，各存儲信息區段之核對值全部無誤。

其次，在步驟 S 5 8 中，記錄再生器 3 0 0 之控制器 3 0 1，併用以取出區段資訊 (D I T) 內之存儲信息區段資訊，並存儲信息區段是否為真驗證對象，使存儲信息區段成為驗證對象時，則在著者之中區段資訊中使存儲信息指標對值無容納。

僅當使用此區段成為驗證對象時，則將該區之存儲信息區段，並用記錄再生器 3 0 0 之錄取部 3 0 4 由庫量 5 0 0 取出，或使用記錄再生器 3 0 0 之進訊部 3 0 5 由道訊號碼 6 0 0 進行接收，並啟動記錄再生器 3 0 0 之記錄再生器指標處理部 3 0 2，將此接收後之記錄再生器指標碼 3 0 2 之控制部 3 0 6，係在記錄再生器指標處理部 3 0 2 之控制部 3 0 6，併存儲信息中間並計算。

存儲信息中間值，係在步驟 S 5 4 以譯碼化後之存儲信息編寫 Kcon，將被輸入之後存儲信息區段以 D E S 之 C B C 條式進行驗證，並將其結果區割成 8 級元，全部達

## 五、發明說明 (116)

其次，步驟 S 5 9 中，記錄再生器 3 0 0 之記錄再生器指標處理部 3 0 2，係在步驟 S 5 4 將進行譯碼化放棄的區段資訊指標 Kbit 及存儲信息指標 Kcon，在記錄再生器指標部 3 0 2 之控制部 3 0 6 與譯碼化部 3 0 8，相互對照時以進行尚未有放棄的對話時間識別 Kts 使用標準化，記錄再生器 3 0 0 之控制部 3 0 1，係所以對話時間識別 Kts 被標準化後之區段資訊指標 Kbit 及存儲信息指標 Kcon 由記錄再生器 3 0 0 之記錄再生器指標部 3 0 2 退出，並將此等之資料將送回記錄再生器 3 0 0 之記錄再生器指標部 3 0 2 以記錄裝置 4 0 0 。

其次，步驟 S 6 0 中，用以接收由記錄再生器 3 0 0 送回來之區段資訊指標 Kbit 及存儲信息指標 Kcon 後之記錄裝置 4 0 0，並將接收後之資料在互聯網傳輸線或總部 4 0 1 之串接埠／譯碼化部 4 0 5，在互聯網時以進行尚未有放棄的對話時間識別 Kts 使用標準化，以保存於記錄裝置指標部 4 0 1 之內部記錄部 4 0 5 的記錄裝置固有保存指標 Kstt 使再標準化。最後，記錄再生器 3 0 0 之控制部 3 0 1，係透過記錄再生器 3 0 0 之記錄再生器指標部 3 0 3，由記錄裝置 4 0 0 以保存指標 Kstt 用以讀出各項資料之後之區段資訊指標 Kbit 及存儲信息指標 Kcon，而且，將此等之指標，以記錄裝置 Kds 廣播成被標準化後之區段資訊指標 Kbit 及存儲信息指標 Kcon。

步驟 S 6 1 中，記錄再生器 3 0 0 之控制部 3 0 1，係由資料之集管部之處理方針 (Usage Policy) 取出利用

## 五、發明說明 (117)

存儲信息指標並加以生成。

記錄再生器指標處理部 3 0 2 之控制部 3 0 6，係在記錄再生器指標處理部 3 0 2 之指標／譯碼化部 3 0 8 使存儲信息指標對值之計算，存儲信息指標，並將被保存於記錄再生器指標處理部 3 0 2 之內部記憶體 3 0 7 的存儲信息指標對值生成為指標 Kicv 故落獨立，將存儲信息中間值以 D E S 進行驗碼化並加以生成。而且，記錄再生器指標或處理部 3 0 2 之控制部 3 0 6，係用以比較該存儲信息指標，及在步驟 S 5 1 由記錄再生器 3 0 0 之控制部 3 0 1 收取之存儲信息區段內的 I C V，並將其結果轉交到記錄再生器 3 0 0 之控制部 3 0 1，將此後收從之記錄再生器 3 0 0 之控制部 3 0 1，係在聯繫進行成功時，用以前次之驗碼對存儲信息區段並以記錄再生器 3 0 0 之記錄再生器指標處理部 3 0 2 之驗碼，用以驗證全部存儲信息區段為此後收同樣的驗碼或否。尚且，若將 Header 生成而核對放棄，則做為 I V = 0，並記錄再生器指標處理部 3 0 2 之內部記錄部 3 0 7 用以保存存儲信息指標對值或用初期值 I V = 數字，將此加以使用也可。又，根據之後之全部的存儲信息指標，係保証於記錄再生器 3 0 0 之記錄再生器指標處理部 3 0 2 放棄。進而，記錄再生器 3 0 0 之記錄再生器指標處理部 3 0 2，以資料轉給驗證對象之存儲信息區段的驗證順序，順序有錯誤，或使用同一存儲信息區段進行 2 次以上驗証時，則做為認定失敗。而且，全部之驗證進行成功時，則達到步驟 S 5 9 。

## 五、發明說明 (119)

記錄資訊，當下載之後之存儲信息用以判定僅以該記錄再生器 3 0 0 可利用 (該情形，利用限制資訊係設定成 1)，或以另開之另開記錄再生器 3 0 0 也可利用 (該情形，利用限制資訊係設定成 0)，判定之結果，利用限制資訊係 1 時，則達到步驟 S 6 2 。

步驟 S 6 2 中，記錄再生器 3 0 0 之控制部 3 0 1，係將記錄裝置固有之指標在記錄再生器 3 0 0 之記錄再生器指標處理部 3 0 2 使計算。記錄裝置固有之指標值，係知識圖 2 5 所述將被保存於記錄再生器指標處理部 3 0 2 之內部記錄部 3 0 7 的記錄再生器指標名稱指 Kdsv 作為指標，在步驟 S 5 8 進行保持放棄的中間對值以 D E S 進行標準化並加以生成。計算後之記錄再生器固有之指標 I C Vds，係代為較核對值 I C V t 之上。

如前面已敘說明，系統署名指標 Ksys，係在記錄系統為附上共同之署名或 I C V 使用之系統署名指標，又，記錄再生器署名指標 Kdev，係在各記錄再生器不同，使記錄再生器有了附上署名或 I C V 使用之記錄再生器署名指標，即非由系統署名指標 Ksys 署名之資料，係由於具有相同系統署名指標的系統 (記錄再生器) 便核成功。即使核對值 I C V t 形成進行一致，所以成為可共用，但使記錄再生器署名指標 Kdev 被署名後時，則記錄再生器署名指標係在其所記錄再生器之固有論點，所以使用記錄再生器署名指標 Kdev 被署名後之資料，即，署名後，被容納於記錄裝置之資料，係在其他之記錄再生器，用以廣泛擴

A7  
B7**五、發明說明 (120)**

記錄装置在欲再生時，以記錄再生器之固有核對碼 ICVdev 形式不一致，形成雜訊所造成為不能再生。

因此，本發明之資料處理裝置中，藉由利用限制資訊之設定，在系統可共同使用存儲信息，在記錄再生器固有時可利用之存儲信息形式可自由設定。

步驟 S 6 3 中，記錄再生器 3 0 0 之控制部 3 0 1，張得存儲信息保存於記錄裝置 4 0 0 之外部記憶體 4 0 2

。圖 2 6 係顯示利用限制資訊在 0 之情形中記錄裝置內之存儲信息狀況圖，圖 2 7 則顯示利用限制資訊在 1 之情形中記錄裝置內之存儲信息狀況圖，圖 2 6 與圖 2 7 不同點，係由於每個存儲信息編號 Kbsi 及存儲信息編號 Kcon 以記述編號 Kbsi 位被暗號化，僅以存儲信息 Kbsi 位被暗號化，又，圖 2 7 與圖 2 6 不同點，係由於因該對值被計算之核對碼，在圖 2 6 係以系統名稱碼 Keys 位被暗號化，相對地在圖 2 7 係以記錄再生器固有之記錄再生器名稱碼 Kdev 位被暗號化。

實有，圖 2 2 之處理過程中，在步驟 S 5 2 對核對碼 A 之驗證進行失敗時，在步驟 S 5 5 對核對碼 B 之驗證進行失敗時，在步驟 S 5 7 對核對碼 C 之驗證進行失敗時，在步驟 S 5 8 對各存儲信息區段之存儲信息核對碼之驗證進行失敗時，則進至步驟 S 6 4，進行預定之錯誤顯示。

又，在步驟 S 6 1 利用限制資訊在 0 之情形，則該過

A7  
B7**五、發明說明 (121)**

步驟 S 6 2 進到步驟 S 6 3。

(8) 以記錄裝置內記錄再生器的再生處理其次以被容納於記錄裝置 4 0 0 之外部記憶體 4 0 2 的存儲信息資訊之記錄再生器 3 0 0 對於再生處理加以說明。

圖 2 8 係用以說明使記錄再生器 3 0 0 由記錄裝置

4 0 0 證出存儲信息，並用以利用存儲信息之程序流程圖

。圖 2 8 中，首先為在記錄再生器 3 0 0 及記錄裝置

4 0 0 之間已彼此互通訊。

步驟 S 7 1 中，記錄再生器 3 0 0 之控制部 3 0 1，係使用記錄裝置識別碼 3 0 3 由記錄裝置 4 0 0 之外部記憶體 4 0 2 證出存儲信息。而，記錄再生器 3 0 0 之控制部 3 0 1，係將記錄裝置內之Header (Header) 部分傳送到記錄再生器 3 0 0 之記錄再生器導航處理部 3 0 2。步驟 S 7 2，係與「(7) 由記錄再生器對記錄裝置下載或從」中已說明之步驟 S 5 2 同樣之處理，從接收保管 (Header) 後之記錄再生器導航處理部 3 0 2 之控制部

3 0 6，在記錄再生器導航處理部 3 0 2 之釋放 / 譯西化部 3 0 8 使核對值 A 與其之處理。核對值 A，係由前面已說明之圖 2 3 所示所被保存於記錄再生器導航處理部 3 0 2 之內部記憶體 3 0 7 的核對值 A 生成於記錄再生器 Keys 位被暗號化。將識別資訊 (Content ID) 及處理方針 (Usage Policy) 作為信息根據在圖 7 已說明之同樣之 I C V 計算方法被計算。

A7  
B7**五、發明說明 (122)**

如前面已說明項對值 A, I C V s，係為了用以驗證識別資訊 (Content ID) 及處理方針 (Usage Policy) 之資訊的核對值，然後將存儲記錄再生器暗號處理部 3 0 2 之內部記憶體 3 0 7 的核對值 A 生成於記錄 Keys 位被暗號化，並識別資訊 (Content ID) 及處理方針 (Usage Policy) 作為信息根據在圖 7 已說明之 I C V 計算方法被計算之核對值 A，並被容納於Header (Header) 內之核對值：I C V s 進行一收後，並被容納於Header (Header) 內之核對值 A 4 0 0 後之識別資訊，通過方無異狀。

其次，步驟 S 7 3 中，記錄再生器 3 0 0 之控制部

3 0 1，係由讓出之後之無主 (Header) 部分取出回授資訊 Kbit 及存儲信息編號 Kcon，並透過記錄再生器 3 0 0 之記錄裝置壓縮部 3 0 3 送達至記錄裝置 4 0 0。用以接收由記錄再生器 3 0 0 送達而來之區段資訊 Kbit 及存儲信息編號 Kcon 後之記錄再生器 4 0 0，並將接收到之資訊於記錄裝置壓縮部 4 0 1 之序號 / 譯碼化部 4 0 6，以保存於記錄裝置壓縮部 4 0 1 之內部記憶體

4 0 5 的記錄裝置固有之存儲編號 Kstr 位被暗號化處理，在相互認證時以進行共有啟動之對話時間指標 Kses 位被暗號化，而且，記錄再生器 3 0 0 之控制部 3 0 1，並透過記錄再生器 3 0 0 之記錄裝置壓縮部 3 0 3，由記錄再生器 4 0 0 以對話時間指標 Kses 位以接出存儲信息編號化後之區段資訊 Kbit 及存儲信息編號 Kcon。

其次，步驟 S 7 4 中，記錄再生器 3 0 0 之控制部

A7  
B7**五、發明說明 (123)**

3 0 1，係以接收後之對話時間指標 Kses 將被再暗號化後之區段資訊編號 Kbit 及存儲信息編號 Kcon 發送至記錄再生器 3 0 0 之記錄再生器導航處理部 3 0 2。

以對話時間指標 Kses 用以接收被再暗號化後之區段資訊編號 Kbit 及存儲信息編號 Kcon 後的記錄再生器 3 0 0 之記錄再生器導航處理部 3 0 2，係在記錄再生器導航處理部 3 0 2 之釋放 / 譯西化部 3 0 8，以對話時間指標 Kses 將被暗號化後之區段資訊編號 Kbit 及存儲信息編號 Kcon，在相互認證時以進行共有啟動之對話時間指標 Kses 位被暗號化，又，以譯西化後之區段資訊編號 Kbit，在步驟 S 7 1 並進行接收啟動的區段資訊被譯西化。

尚有，記錄再生器 3 0 0 之記錄再生器導航處理部 3 0 2，係將被暗號化後之區段資訊編號 Kbit，存儲信息編號 Kcon 及區段資訊 B I T，在步驟 S 7 1 亂換成接收啟動的區段資訊編號 Kbit，存儲信息編號 Kcon 及區段資訊 B I T 並加以保持啟動。又，記錄再生器 3 0 0 之控制部 3 0 1，係將被暗號化後之區段資訊 B I T 送達記錄再生器 3 0 0 之記錄再生器導航處理部 3 0 2 亂換成啟動。

步驟 S 7 5，係與「(7) 由記錄再生器對記錄裝置下載或從」中已說明之步驟 S 5 6 同樣之處理，使記錄再生器首尾端號處理部 3 0 2 之控制部 3 0 6，由記錄裝置 4 0 0 賦予之後之區段資訊編號 Kbit，存儲信息編號 Kcon 及區段資訊 B I T 分割成 8 組元尾序，並將此等全部進行譯西化處理。其次，記錄再生器組號處理部 3 0 2

A7

B7

**五、發明說明 (124)**

之記錄再生器當場號處理部 3 0 2 之暗號／譯碼機 3 0 8 便核對值 B ( I C V b ) 計算。核對值 B，係如前若已說明所指，將被保持於記錄再生器暗號號處理部 3 0 2 之內部記錄 3 0 7 的核對值 B 生成輪點 Kicvb 並為論點，將所才計算後之推進性邏輯和以 D E S 進行印試化並加以生成。最後，用以比較核對值 B 及 Header 內之 I C V b ，進行一一致後時，則被

如前而已說明，核對值 B 、 I C V b 係為了驗證區段資訊而存於 Kicvb 在記錄再生器暗號號處理部 3 0 2 之內部記錄 3 0 7 的核對值 B 生成輪點 Kicvb 並為論點，由記錄再生器 4 0 0 所譯出之後之區段資訊而存於 Kicvb，在記錄再生器暗號號處理部 3 0 2 分別成 8 級單元並進行推進性邏輯和，若得條件以 D E S 進行輪點化並生成之後之核對值 B ，與若啟動於記錄再生器 4 0 0 譯出之後之資料中的素質 ( Header ) 之核對值 I C V b 進行一致後時，則被判斷地將於記錄再生器 4 0 0 之後的資料的區段資訊而存於 Kicvb，在記錄再生器暗號號處理部 3 0 2 之內部記錄 3 0 7 中。

步驟 S 7 6 中，記錄再生器當場號處理部 3 0 2 之控制部 3 0 6 ，係在記錄再生器暗號號處理部 3 0 2 之暗號／譯碼化部 3 0 8 便中記錄對應計算，中間核對值，並如前若已說明第 2 5 所示將被保存於記錄再生器暗號號處理部 3 0 2 之內部記錄 3 0 7 的核對值生成輪點 Kicvt 並為論點，將被核對後之素質 ( Header ) 內之核對值 A 、核對值

本辦法適用於中國國家標準 ( CNS ) 标誌 ( 210 = 297 公里 ) - 127 -

A7

B7

**五、發明說明 (125)**

B 、進行保持放著之全部的存儲信息核對值作為信息相識圖 7 已說明之 I C V 術算方法進行計算。現有，做為初期値係 I V T = 0 。在記錄再生器當場號處理部 3 0 2 之內部記錄 3 0 7 用以保存被稱為生成用初値值 I V T 依著，將此進行使用也可。又，生成後之中間核對值，依循必要保持記錄再生器 3 0 0 之記錄再生器暗號號處理部 3 0 2 放著。

接著，步驟 S 7 7 中，記錄再生器 3 0 0 之控制部 3 0 1 ，係由記錄再生器 4 0 0 之外部記憶體 4 0 2 被合於下載後之資料的集存地而處理方針 ( Usenet Policy ) 有看出利用限制資訊，使下載後之存儲信息進行判斷並可利用該記錄再生器 3 0 0 ( 利用限制資訊為 1 ) ，或也可利用另外同樣之記錄再生器 3 0 0 ( 利用限制資訊為 0 ) 、判定之結果，利用限制資訊為 1 ，即下載後之存儲信息誰可利用該記錄再生器 3 0 0 被規定定期制限時，則達到步驟 S 8 0 ，而利用限制資訊為 0 ，即也可利用另外同樣之記錄再生器 3 0 0 之規定時，則達到步驟 S 7 8 。尚有，步驟 S 7 7 之處理，依使被核對值部 3 0 2 進行也可。

步驟 S 7 8 中，係 ( 7 ) 由記錄再生器部對記錄再生器之下載處理中與已說明之步驟 S 5 8 被執行同樣之核對值 I C V l 的計算，即，記錄再生器暗號號處理部 3 0 2 之控制部 3 0 6 ，係在記錄再生器當場號處理部 3 0 2 之暗號／譯碼化部 3 0 8 處理核對值 I C V t 之計算，將核對值 I C V t ，係如前面已說明之圖 2 5 所示將被保存於記錄再生器當場號處理部 3 0 2 之內部記錄 3 0 7 中。

本辦法適用於中國國家標準 ( CNS ) 标誌 ( 210 = 297 公里 ) - 128 -

A7

B7

**五、發明說明 (126)**

再生器當場號處理部 3 0 2 之內部記錄 3 0 7 的系統筆名編號 Ksys 依循地此，將中間核對值以 D E S 進行輪點化並加以生成。

其次，進到步驟 S 7 9 ，用以比較步驟 S 7 8 中之生成後之絕對值 I C V t 及在步驟 S 7 1 進行保存放著的素質 ( Header ) 內之 I C V t ，進行一致後時，則達到步驟 S 8 2 。

如前而已說明，總核對值 I C V t ，係為了用以驗證 I C V a 、 I C V b ，各存儲件也甚於之核對值全部之來成後的絕對值。因此，藉上述之過程被生成之後之總核對值與其容於之素質 ( Header ) 內之核對值： I C V t 進行一致後時，則啟動於記錄再生器 4 0 0 之後的資料中，被判斷 I C V a 、 I C V b ，各存儲件也甚於之核對值全部被生成。

在步驟 S 7 7 之判定中，若是進行下載之存儲信息僅可利用該記錄再生器 3 0 0 之設定時，即設定資訊為 1 時，則達到步驟 S 8 0 。

步驟 S 8 0 中，記錄再生器當場號處理部 3 0 2 之控制部 3 0 6 ，係在記錄再生器當場號處理部 3 0 2 之暗號／譯碼化部 3 0 8 ，使記錄再生器當場號有之核對值 I C V d e v 之計算。記錄再生器當場號有之核對值 I C V d e v ，係如前面已說明之圖 2 5 所示將被保存於記錄再生器當場號處理部 3 0 2 之內部記錄 3 0 7 的記錄再生器當場號有之默認再生器筆名編號 Kdev 並為論點，將中間核對值以 D E S 進行輪點化並加以生成

本辦法適用於中國國家標準 ( CNS ) 标誌 ( 210 = 297 公里 ) - 129 -

A7

B7

**五、發明說明 (127)**

步驟 S 8 1 中，用以比較在步驟 S 8 0 進行計算後之記錄再生器當場號有之核對值 I C V d e v 及在步驟 S 7 1 進行保存放著的 Header 內之 I C V d e v 在進行一致後時，則達到步驟 S 8 2 。

如此，藉由系統筆名編號 Ksys 被譽名之資料，係藉由具有同系統筆名編號此之系統 ( 記錄再生器 ) 成功核對，即使總核對值 I C V t 之形成進行一致所以成為可利用，並就用記錄再生器當場號 Kdev 被譽名時，即記錄再生器當場號筆名地處在其記錄再生器具有而有之論點，所以使用記錄再生器當場號 Kdev 被譽名之資料，即，著名後，被看顧於記錄後置之資料，係在某之其之記錄再生器，用以看著該記錄後置成再生時，使記錄再生器能有之核對值 I C V d e v 形成不一致，形成錯誤是以成為不能再生。因此，藉由利用限制資訊之設定，在此就可使用存儲信息，博可利用於記錄再生器當場號之存儲信息或可自由設定。

步驟 S 8 2 中，記錄再生器 3 0 0 之控制部 3 0 1 ，係在步驟 S 7 4 用以取出進行讓出放著的基級資訊 1 T 之存儲信息區段資訊，並使存儲信息區段資訊是否為等號化對象，成為轉化對象時，將該存儲信息區段，透過記錄再生器 3 0 0 之紀錄新舊控制部 3 0 3 ，由記錄再生器 4 0 0 之外部記憶體 4 0 2 進行廣出，並使對記憶再生器 3 0 0 之記錄再生器當場號處理部 3 0 2 、博可接收後之記錄再生器當場號處理部 3 0 2 之控制部 3 0 6 ，係在記錄再生器當場號處理部 3 0 2 之津號／譯碼化部 3 0 8 使存

本辦法適用於中國國家標準 ( CNS ) 标誌 ( 210 = 297 公里 ) - 130 -

A7  
B7

## 五、發明說明 (128)

俾存儲信息過化，同時使存儲信息區段成為驗證對象時而在下次之步驟 S 8 3 中使用存儲信息核對值進行驗証。

步驟 S 8 3 中，係與「(7)」由記錄再生器對記錄裝置之存儲信息區段中已接收到之步驟 S 5 6 同樣之處理。記錄再生器 3 0 0 之控制部 3 0 1，係用以取出各段資訊 (B 1 T) 內之存儲信息區段資訊，將存儲信息區段是否成為驗證對象由存儲信息核對值之新狀況進行判定，使存儲信息區段成為驗證對象時，則該存儲信息區段，由記錄裝置 4 0 0 之外部記憶體 4 0 2 進行接收，並發送紀錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2。其後接收後之記錄再生器帶號碼處理部 3 0 2 之控制部 3 0 6，係在記錄再生器帶號碼處理部 3 0 2 之類號／譯碼化部 3 0 8 使存儲信息區段進行計量。

存儲信息中間值，係在步驟 S 7 4 以譯碼化後之存儲信息輸給 Keon，將接輸入後之存儲信息區段以 DES 之 CBC 模式進行詳密化，將其結果重新組成 8 位元全部進行辨識細節和並加以生成。

其次，記錄再生器帶號碼處理部 3 0 2 之類號／譯碼化部 3 0 8 係存儲信息核對值進行計算，存儲信息核對值，係將存儲於記錄再生器帶號碼處理部 3 0 2 之外部記憶體 3 0 7 的存儲信息核對值生成輸給 Kicte 作為輸出，並將存儲信息中間值以 DES 進行譯碼化並加以生成。而且，記錄再生器帶號碼處理部 3 0 2 之控制部 3 0 6，係用以比較

A7  
B7

## 五、發明說明 (129)

該存儲信息核對值，及在步驟 S 7 1 由記錄再生器 3 0 0 之控制部 3 0 1 接收後之存儲信息區段內之 I C V，並将其結果轉寫到記錄再生器 3 0 0 之控制部 3 0 1。將此接收後之記錄再生器 3 0 0 之控制部 3 0 1，係在驗證進行成功後時，所以取出下次驗證對象存儲信息區段並在記錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2 之類號化，用以驗證全部存儲信息區段為止重複同樣之較正過程，尚有：初期值係依於 I V = 0，在記錄再生器帶號碼處理部 3 0 2 之外部記憶體 3 0 7 用以保存存儲信息核對值生成用初值 I V = 0，將此進行使用也可。又，類號後之全部的存儲信息對照時，係保持於記錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2 故著，繼而又，記錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2，係用以監視驗證對象之存儲信息並接收到驗證順序，使順序跳躍，或將同一之存儲信息區段使 2 次以上前後時，則做為進行認定失敗。

記錄再生器 3 0 0 之控制部 3 0 1，係用以接收該存儲信息核對值之比較結果（未成為驗證對象時，則比較結果係全部做為成功），在驗證進行成功後時，則由記錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2 取出被譯碼化之後之存儲信息，而且，所以在此下次擇選存儲信息區段並在記錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2 使譯碼化，將全部之存儲信息區段進行譯碼停止後進行

A7  
B7

## 五、發明說明 (130)

尚有，在步驟 S 8 3 中，記錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2，係在存儲信息核對值之驗證處理中形態不一致時，則假設被輸入放在該步驟用以中止處理，而剩下存儲信息之譯碼化所不進行。又，記錄再生器 3 0 0 之記錄再生器帶號碼處理部 3 0 2，係用以就說譯碼化對象之存儲信息區段的譯碼化順序，從順序有錯誤，或將同一之存儲信息區段使 2 次以上進行譯碼化時，則依據為進行譯碼化失敗。

尚有，在步驟 S 7 2 係將 A 之驗証進行失敗時，在步驟 S 7 5 係將 B 之驗証進行失敗時，在步驟 S 7 9 係將對值 I C V 之驗証進行失敗時，在步驟 S 8 1 係記錄再生器 3 0 0 各存儲信息區段之存儲信息核對值進行驗証時，在步驟 S 8 3 各存儲信息區段之存儲信息核對值進行驗証時，則達到步驟 S 8 4，進行最後之階段顯示。

如以上所敘的說明，將存儲信息進行下載，或進行利用時，將重要的資料或存儲信息進行量化後並進行譯碼化，不儘可宣驗驗証，而且以譯碼化後資訊將 B 1 T 之區段資訊轉換成 Kbit，爲了用以譯碼化存儲信息之資料，Keon 係以記錄裝置指出之具有存儲點 Kbit 因爲被保存，所以單別將記錄裝置上之資料在到的記錄裝置進行複製，也即將存儲信息不能正確的進行譯碼化，更其種而言，譬如圖 2 之步驟 S 7 4 中，將有在各記憶以不同保存編號 Kbit 為了用以譯碼化並能將其之資料，以到的記錄裝置作為資料不能正確譯碼化之構成。

A7  
B7

## 五、發明說明 (131)

## (9) 相互認証後之歸還交換處理

本發明之資料處理装置中特徵之一，係在上述之記錄再生器 3 0 0 及記錄裝置 4 0 0 之間僅在被執行時及認証處理之後，纔可將記錄裝置之利用，又，進行添附其利用照樣之點。

譬如，由於不當重複等用以生成容納存儲信息後之記錄卡等之記錄裝置，將此設定於記錄再生器為了將該被利用，在記錄再生器 3 0 0，及記錄裝置 4 0 0 間執行相互認証處理，且將該成認証 OK 作為條件，在存儲信息 (已被譯碼化) 之記錄再生器 3 0 0 及記錄裝置 4 0 0 間當為可傳達。

爲了用以實現上述之限制的處理，本身具之資料處理裝置中，係在記錄裝置 4 0 0 之時間處理部 4 0 1 時，全部，形成稱或根據被預先設定後之指令判別被執行，即，記錄裝置，係具有根據指令號碼將指令由順序存儲取出並執行之功能而構成，圖 2 係顯示以該記錄裝置用以說明指令成因塊圖。

如圖 2 所示在具有記錄再生器帶號碼處理部 3 0 2 之記錄再生器 3 0 0 及具有記錄裝置帶號碼處理部 4 0 1 之記錄裝置 4 0 0 間，在記錄再生器 3 0 0 之控制部 3 0 1 的直接下制由記錄裝置產生於 3 0 3 由記錄裝置 4 0 0 之資訊部 (含接收存儲器) 4 0 4 使用令號碼被輸出。

記錄裝置 4 0 0，係在帶號碼處理部 4 0 1 內之控制部



**五、發明說明 (136)**

訊號化 Kbit，存儲信息編址 Kcon) 的譯出之步驟。

步驟 S 3 1 0 2，係由記錄裝置之記錄儀以譯出之後之存儲地址 Kstr 將被標號化後之資料 (e.g. 評審資訊編址 Kbit，在存儲信息編址 Kcon) 容納於其存儲之步驟。該步驟中，係由記錄裝置 4 0 0 之外部記憶體 4 0 2 使記錄再生器 3 0 0 以保存地址 Kstr 用以譯出後標號化後之資料，在其後此步驟的記錄裝置 4 0 0 之寄存器也可。

步驟 S 3 1 0 3，係以保存地址 Kstr 將被標號化後之資料 (e.g. 評審資訊編址 Kbit，在存儲信息編址 Kcon) 由寄存器釋出並以保存地址 Kstr 進行譯換或處理之步驟。

步驟 S 3 1 0 4，係以保存地址 Kstr 將被標號化後之資料 (e.g. 評審資訊編址 Kbit，在存儲信息編址 Kcon) 以對話時間點 Kstt 進行時間數字化處理之步驟。

上列之處理步驟 S 3 1 0 2 ~ S 3 1 0 4，係結合於前述圖 2 9 0 之發令寄存器中之指令碼而  $\mu-y$  的處理。此等之處理，係記錄裝置之指令碼為步驟 2 9 0 1 中由紀錄再生器 3 0 0 核據釋收之指令碼而  $\mu-y$  以記錄再生器 3 0 0 依序順序執行。

其次之步驟 S 3 1 0 5，係以對話時間點 Kstt 將被標號化後之資料 (e.g. 評審資訊編址 Kbit，在存儲信息編址 Kcon) 由記錄裝置進行譯換並把錄再生器釋出。

上列之步驟 S 3 1 0 2 ~ S 3 1 0 4，係僅限被執行不可插入的執行序列，譬如，在步驟 S 3 1 0 3 之記錄裝置終了時點，由記錄再生器 3 0 0 即將有資料譯出指令。

本領域大抵適用中國國家標準 (CNISIA) 第 201~207 公量。 - 159 -

**五、發明說明 (136)**

係不適用於上述圖 4 所示之格式，使得各個信息有其獨特之情形，有圖參照之情形，遊戲等之程式的情形等，根據存儲信息用以採用資料格式或模式，以下，對於複雜之不同的資料格式，及對應於各格式所對記錄裝置之下載處理及由記錄裝置之再生過程加以說明。

圖 3 2 ~ 3 5 係顯示 4 不同的資料格式，在各區之左側，係顯示圖 3 所示導讀器 5 0 0 或導讀裝置 6 0 0 中之資料形式，又在各區之右側係顯示被容納於記錄裝置 4 0 0 之外部記憶體 4 0 2 中之資料格式。首先，用以說明圖 3 2 之資料形式或之結構，之後，對於各格式之中之各資料之內容，及各格式之中之資料的差異加以說明。

圖 3 2，係格式形態 0，在上述之說明中既已經顯示之形式，及共同形態，該格式形態之特徵，係將資料全體分割成任意大小的 N 個之資料子段，即分割成區段 1 ~ 區段 N，對於各區段往來進行譯換時，可構成串接化區段及串接化區段，即，從機上平行來看可構成資料之點。首次串接化，係藉由存儲信息編址 Kcon 係執行，在記錄裝置中容納於 Kcon，係在基體上藉由記錄裝址 Kbit 被標號化，在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記錄儀之保存地址的存儲地址 Kstr 被標號化，對於區段資訊編址 Kbit 也在基體上藉由記錄裝址 Kstr 被標號化，在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記錄儀之保存地址 Kstr 被標號化，此互之標號化，係根據前述之「(9) 相互証記之後之標號化及處理」中說明之處理被執行。

本領域大抵適用中國國家標準 (CNISIA) 第 201~207 公量。 - 141 -

**五、發明說明 (137)**

但其譯出指令，係因為而被設定於指令地址 2 9 0 2 之指令號而  $\mu-y$  的發令序列指令號不同，所以指令碼管理器 2 9 0 1，係不接收譯出之執行，因此記錄裝置 4 0 0 中之記錄交換將產生之譯換資料由外部，譬如由記錄再生器 3 0 0 形成不可譯出，可防止據此資料，存儲信息之不正常的譯出。

尚有，圖 3 0 ~ 3 1 所示之處理，係單由錄底交換使被譯換，當量化對象，顯示有西段資訊編址 Kbit，在存儲信息編址 Kcon 之例，但被容納於此等之圖 2 9 0 所示之西段寄存器 2 9 0 2 之標號化序列，係僅僅存儲信息由錄底及交換合有譯換，而量化處理也可，藉由錄底交換使被譯換，標量化對象係並非固定於上述之例。

以上，對於不舉明之資料或記錄裝置中相互通訊後的錄底交換處理做了說明，如此，本發明之資料或記錄裝置中之錄底交換處理，係在記錄再生器及記錄裝置間僅在終了記錄處理後方為可執行，而前，由錄底交換處理中之深層資料的外部分可防止取用的構成，所以僅存儲信息，量化資料之高度的安全性被保證。

(10) 數字之存儲信息格式，及對應於各格式的下載及再生處理

上述之實施例，係譬如使用圖 3 所示導讀器 5 0 0 或導讀裝置 6 0 0 中之資料格式對圖 4 所示 1 種的情形做了說明，可是，據圖 5 0 0 或導讀裝置 6 0 0 中之資料格式，

本領域大抵適用中國國家標準 (CNISIA) 第 201~207 公量。 - 140 -

**五、發明說明 (139)**

圖 3 3，係格式形態 1，該資料形態 1，係與格式形態 0 同樣，將資料主體分割成 N 個之資料區段，部分劃成區段 1 ~ 區段 N，將各區段之名區段之大小設為同樣大小之點與前述格式形態 0 不同。藉由存儲信息編址 Kcon 使區域之標號化處理像係在前述之格式形態 0 同樣，又，在基體上藉由記錄裝址 Kstr 被標號化，在記錄裝置中之保存時係藉由被容納於記錄裝置之內部記錄儀之保存地址 Kstr 被標號化存儲信息編址 Kcon 及區段資訊編址 Kbit 構成也與上述格式形態 0 同樣，格式形態 1，係與格式形態 0 不同，係因為固定性的區段而成，使各區段之資料長度等之導讀資料被標號化，所以相比格式形態 0 成活可減少區段資訊之記錄體積大小。

圖 3 3 之構成例，係將各區段藉由標號化部分及非標號化部分 (不常文) 之 1 次進行構成，如此區段之具備，被構成有規則性，則在譯換處理時各區段共度，而並不需要以選擇區段構成所以成為可有效譯換，惟據處理，尚有，在格式 1 中，用以構成各區段之部分，即標號化部分或，非標號化 (不常文) 部分，係在各部分構成為標有其型態或可定義的構成，如要較快製作之基底時，係藉於其基底之存儲信息核對碼 I C V 1 之定義。

圖 3 4，係格式形態 2，該格式形態 2 之特徵，係同樣大小之 N 個之資料寬度，即被分割成區段 1 ~ 區段 N，對於各區段，分別以個別之區段地址 Kbit 被標號化，各區段地址 Kbit，係在基體上藉由記錄裝址 Kstr 被標號化，在

本領域大抵適用中國國家標準 (CNISIA) 第 201~207 公量。 - 142 -

五、發明說明（<sup>140</sup>）

記錄裝置中之保存時，係將由寄納於記錄被授權之內部記憶體後之保存編號 Ktr 被轉號化。對於基底資訊編號 Khi 也在媒體上和由記憶體編號 Kdi 被轉號化，在記錄裝置中之保存時，係將由寄納於記錄裝置之內部記憶體後之保存編號 Ktr 被轉號化。

圖 3-5，係格式形態 3，該格式形態 3 之特點，係與格式形態 2 同樣，因欄大小之 N 個之資料欄位，即被分割成區段 1 ~ N 區段 N，對於各區段，分別以分別之基底資訊編號 Khi 被轉號化，並非一併使用存儲信息編號，各區段資訊編號 Khi 在媒體上藉由記憶體編號 Kdi 被轉號化，在記錄裝置中之保存時，係將由寄納於記錄裝置之內部記憶體後之保存編號 Ktr 被轉號化。

其次，對於上述格式形態 0 ~ 3 之資料內容而言以說明，資料係如前述之級別，被分為基底資訊及存儲信息兩大類，其管部係會有存儲信息識別子，或指方針，依對號 A、B、總指對號，而設資訊識別，存儲信息識別，基底資訊。

就現行方式，存儲信息之資料長，無齊齊，格式形態（以下所說之格式形態 0 ~ 3），譬如存儲式、資料等之存儲信息形態，對前述之存儲信息之記錄被識別的下標，如再生之標的說明，使存儲信息用以決定在記錄再生基底

本說明文字適用於中國國家標準（GB/T15446-2001）第 20~297 企業） - 143 -

五、發明說明（<sup>142</sup>）

係底資訊被轉號化時，將平原文（譯英文）全體以 8 組元單位轉進行非連續性和之值從被寄納於記錄再生器

3 002 內的記憶體 3 07 之後之字傳到被寄納於底資訊編號 Kive 做為轉號化之值被生成。又，區段未被轉號化時，則將區段資料（平原文）之全體以 8 組元單位輸入於圖 3-6 所示資訊改換器生成函數（D R-S-C B C-M A C），將存儲信息編號對值生成編號 Kive（即存儲點）做為取得之值被生成。圖 3-3 係顯示用以生成存儲信息底資訊編號之各 8 組元。

尚有，在格式形態 1 中，係將區段內之零件中至少 1 個存儲對值 I C V 1 之對象資料，即要對零件時，則有算算結果並存儲存儲信息編號 I C V 1。區段中之零件之零件對值 P-I C V 1，即零件 P 之轉號化時，將平原文（譯英文）全體以 8 組元單位進行非連續性和之值以存儲信息底資訊生成編號 Kive 做為進行轉號化之後之值被生成。又，使零件 P 之零件被轉號化時，將零件之區段資料（平原文）的全體以 8 組元單位輸入於圖 3-6 所示資訊改換器生成函數（D R-S-C B C-M A C），將存儲信息底資訊生成編號 Kive（即存儲點）做為取得之值被生成。

進而，在 1 個區段 1 內顯示有枝對對象 I C V 標記 = subject of I C V 之零件，即要對零件 P 之存在時，則以上述方法將生成後之值對值 P-I C V 1 被存儲於區段之零件 I C V 1。又，在 1 個區段 1 內顯示有枝對對象（

五、發明說明（<sup>141</sup>）

有者可利用之標記之複部性標記，進而，存儲信息之複製，有關移動或處理之許可標記，進而，存儲信息簡化計算法，模式等，用以寄納有存儲信息之各種的利用俱制資訊及處理資訊。

核對號 A： I C V a，係對識別資訊，處理方針之核對號，譬如，藉由指代變更 2 3 說明之方法被生成。

區段資訊識別 Khi，係為了用以簡化區段資訊之複製，如前面之說明，在媒體上藉由記憶體編號 Kdi 被轉號化，在記錄裝置中之保存時，藉由並寄納於記錄裝置之內部記憶體後之保存編號 Ktr 被轉號化。

存儲信息識別 Keo，係使用的存儲信息之識別，格式形態 D、I，係與資訊資訊編號 Khi 同樣在媒體上藉由記憶體編號 Kdi 被轉號化，在記錄裝置中之保存時，藉由被寄納於記憶體後之內部記憶體後之保存編號 Ktr 被轉號化，尚有，在格式形態 2，存儲信息識別 Keo，被構成於存儲信息區段在底資訊編號 Khi 之轉號化也位被利用。又，格式形態 3 中，存儲信息識別 Keo 係不存在。

區段資訊，係所以記憶體中之資訊資訊的標識，區段之大小，對於是否被轉號化之標記，即顯示各區段是否形成或核對對象（I C V ）被寄納資訊，區段形成或核對對象時，即隨區段之核對值 I C V i（區段 i 之核對值）在某項中是是並被容許，該區段資訊，係藉由基底資訊識別 Khi 被轉號化。

尚有，區段之核對值，即每個信息核對值 I C V i，

本說明文字適用於中國國家標準（GB/T15446-2001）第 20~297 企業） - 144 -

五、發明說明（<sup>142</sup>）

係底資訊被轉號化時，將平原文（譯英文）全體以 8 組元單位轉進行非連續性和之值從被寄納於記錄再生器

3 002 內的記憶體 3 07 之後之字傳到被寄納於底資訊編號 Kive 做為轉號化之值被生成。又，區段未被轉號化時，則將區段資料（平原文）之全體以 8 組元單位輸入於圖 3-6 所示資訊改換器生成函數（D R-S-C B C-M A C），將存儲信息底資訊編號對值生成編號 Kive（即存儲點）做為取得之值被生成。圖 3-3 係顯示用以生成存儲信息底資訊編號之各 8 組元。

尚有，在格式形態 1 中，係將區段內之零件中至少 1 個存儲對值 I C V 1 之對象資料，即要對零件時，則有算算結果並存儲存儲信息編號 I C V 1。區段中之零件之零件對值 P-I C V 1，即零件 P 之轉號化時，將平原文（譯英文）全體以 8 組元單位進行非連續性和之值以存儲信息底資訊生成編號 Kive 做為進行轉號化之後之值被生成。又，使零件 P 之零件被轉號化時，將零件之區段資料（平原文）的全體以 8 組元單位輸入於圖 3-6 所示資訊改換器生成函數（D R-S-C B C-M A C），將存儲信息底資訊生成編號 Kive（即存儲點）做為取得之值被生成。

進而，在 1 個區段 1 內顯示有枝對對象 I C V 標記 = subject of I C V 之零件，即要對零件 P 之存在時，則以上述方法將生成後之值對值 P-I C V 1 被存儲於區段之零件 I C V 1。又，在 1 個區段 1 內顯示有枝對對象（

五、發明說明（<sup>143</sup>）

I C V 標記 = subject of I C V i) 之零件係觀點存在時，則將被視之零件核對值 P-I C V i) 以選被視之零件號碼順序之資料檢索對值以 8 組元單位輸入於圖 3-7 所示單致模對值對值或函數（D E S-C B C-M A C），將存儲信息底資訊對值生成編號 Kive（即存儲點）做為取得之值被生成。圖 3-7 係顯示用以生成存儲信息底資訊底資訊對值 I C V i) 的構成例。

尚有，格式形態 2、3 中，區段之核對值 I C V i) 係未被定義。

核對值 B： I C V b，係對區段資訊識別，存儲信息識別，新資訊資料之核對值，譬如，在前述圖 2-4 當由說明之方法被生成。

總核對值 I C V i)，係將上述之核對值 A： I C V a，核對值 B： I C V b，進而對被合於形成存儲信息之核對對象的各區段核對值 I C V 1 之核對值，如前述圖 2-5 之說明由核對值 A： I C V a 等之各核對值在被生成中間核對值通用系統等名稱及 Keys 係用以執行階級化處理被生成。

尚有，格式形態 2、3 中，總核對值 I C V i)，係在前述之核對值 A： I C V a，核對值 B： I C V b 存儲信息資料，即由區段 1 之區段編號對值後區段為止由用以選擇存儲信息資料後之資料在被生成中間核對值通用系統等名稱 Keys 係用以執行階級化處理被生成。圖 3-8 係顯示用以生成格式形態 2、3 中之總核對值 I C V i) 的構成例。

本說明文字適用於中國國家標準（GB/T15446-2001）第 20~297 企業） - 145 -

A7  
B7

## 五、發明說明（144）

用有根指標 I C V d e v , 係使前述之局部化標記被設定於 1 時，即，存儲信息顯示在記錄再生器內可供利用時，該置換成根據對值 I C V a 之根對值，格式形態 1 或 2 時，係將該之根對值 A : I C V a ；根對值 : I C V b , 並面對被合於形成存儲信息之根對象的各級根對值 I C V i 全體修改為該對值被生成。其總計步驟，第前進圖 2.5、次圖 3.8 之說明由根對值 : I C V a 等之各級別值在被生成中間根對值識用記錄再生器名稱此 Kdev 藉由以執行規範化處理被完成。

其次在格式形態 0 ~ 3 各次由中由記錄再生器 300 與記錄再生器 400 之存儲信息的下載處理，及對於記錄再生器 300 中由記錄再生器 400 之再生處理使用圖 3.9 ~ 4.4 之流程圖加以說明。

首先，對於格式形態 0、1 中之存儲信息的下載處理，使用圖 3.9 加以說明。

圖 3.9 所示處理，係當加在記錄再生器 300 須由用以裝置記錄裝置 400 之開始時，步驟 S 101，係在記錄再生器及記錄裝置間之認證過程步驟，依據前面說明之圖 2.0 的認證處理流程被執行。

步驟 S 101 之認證處理後，並使認證標記被設定，則記錄再生器 300，係當步驟 S 102 中，暫且由用以容納存儲信息資料之媒體 500，通過讀取部 304 以擇出根據預定之格式的資訊，或使用過載部 305 由匯訊裝置 600 用以接收根據預定之格式的存儲信息，並

A7  
B7

## 五、發明說明（145）

追加。記錄再生器被處理部 302 之控制部 306，係使用記錄再生器名稱此處理部 302 之權限／譯碼化部 308，並使用生成後之記錄識點 Kdis，該造選取部 304 由後收後之僅僅 500，或藉過載部 305 由匯訊裝置 600 進行存儲信息將被接收後之資料的集當部之基底資訊識點 Kbit 及存儲信息識點 Kcon 的譯碼化處理。

進而，步驟 S 107 中，記錄再生器被處理部 302 之控制部 306，係在記錄再生器被處理部 302 之權限／譯碼化部 308 中，以譯碼化後之基底資訊識點 Kbit，將由該資訊識點 Kbit 用以譯碼化般資訊。

進而，步驟 S 108 中，記錄再生器被處理部 302 之控制部 306，係由啟動資訊識點 Kbit，存儲信息識點 Kcon 及基底資訊 (B I T ) 用以生成根據 B ( I C V b ) 之根對值 B , 係如圖 2.4 所示，將被保存於記錄再生器被處理部 302 之內部記錄識點 307 的根對值 B 生成識點 Kicb 作為識點，將由該資訊識點 Kbit，存儲信息識點 Kcon 及基底資訊 (B I T ) 所構成之操作性與 D E S 進行規範化並加以生成。其次，步驟 S 109 中，用以比較根對值 B 及識點 ( Header ) 內之 I C V b ，進行一枚狀跡則跳至步驟 S 110 。

A7  
B7

## 五、發明說明（146）

使記錄再生器 300 之控制部 302，將資訊內之集當 ( Header ) 部分識到記錄再生器 300 之記錄再生器說明為識點 302 。

接著，步驟 S 103 中，使記錄再生器被處理部 302 之控制部 306 在記錄再生器被處理部 302 之權限／譯碼化部 308 使根對值 A 進行計算，根對值 A，係如圖 2.3 所示，將被保存於記錄再生器被處理部 302 之內部記錄識點 307 的根對值 A 生成識點 Kicva 作為識點，並將識點資訊 ( Content ID ) 及處理力計 ( Usage Policy ) 依舊信息根據被使用了之說明的 I C V 計算方法被計算，依舊信息根據被使用了之說明的 I C V 計算方法被計算，步驟 S 104 中，用以比較根對值 A 及被容納於集當 ( Header ) 內之根對值 : I C V a , 在進行一枚時則跳至步驟 S 105 。

如前面說明之根對值 A : I C V a , 係為了用以驗証識點資訊，處理力計之更改的根對值，將被存儲於記錄再生器被處理部 302 之內部記錄識點 307 的根對值 A 生成識點 Kicva 作為識點，將識點資訊 ( Content ID ) 及處理力計 ( Usage Policy ) 作為信息，要使用根據 I C V 計算方法被計算之根對值 A , 與被容納於集當 ( Header ) 內的根對值 : I C V a 進行一枚時，則被判斷異常資訊，處理方法將無效。

其次，步驟 S 105 中，記錄再生器被處理部 302 之控制部 306，係使記述識點 Kdis 之取出或生成在記錄再生器被處理部 302 之權限／譯碼化部 308

A7  
B7

## 五、發明說明（147）

並前而已說明，根對值 B : I C V b , 係為了用以驗証識點資訊識點 Kbit，存儲信息識點 Kcon，基底資訊的篡改之根對值，將被保存於記錄再生器被處理部 302 之內部記錄識點 307 的根對值 B 生成識點 Kicb 作為識點，將資訊識點 Kbit，存儲信息識點 Kcon 及基底資訊 ( B I T ) 分割為 B 及基底資訊並進行操作性辨識與被取得之識點以 D E S 進行規範化後或之後之根對值 B , 被容納於集當 ( Header ) 內之根對值 : I C V b 一較後時，則被判斷資訊識點 Kbit，存儲信息識點 Kcon，基底資訊無篡改。

步驟 S 110 中，記錄再生器被處理部 302 之控制部 306，係在記錄再生器被處理部 302 之權限／譯碼化部 308 中，根據對值 A 之根對值 A , 根對值 B , 進行保持啟者之全部的存儲信息識點對值為根對值 A 之其他根對值之 I C V 計算方法進行計算。尚有，並在之後中間該對值，係根據必要與待於記錄再生器 300 之記錄再生器被處理部 302 放置。

其次，步驟 S 111 中，記錄再生器被處理部 302 之控制部 306，在記錄再生器被處理部 302 之權限／譯碼化部 308 使根對值 I C V b 之計算，根據對值 I C V b , 係如圖 2.5 所示，將被保存於記錄再生器被處理部 302 之內部記錄識點 307 的根對值 B 生成識點 Kicb 作為識點，將資訊識點 Kbit，存儲信息識點 Kcon 及基底資訊 ( B I T ) 用以生成根據 B ( I C V b ) 之根對值 B , 係如圖 2.4 所示，將被保存於記錄再生器被處理部 302 之內部記錄識點 307 的根對值 B 生成識點 Kicb 作為識點，將由該資訊識點 Kbit，存儲信息識點 Kcon 及基底資訊 ( B I T ) 所構成之操作性與 D E S 進行規範化並加以生成。其次，步驟 S 112 中，用以比較根對值 B 及識點 ( Header ) 內之 I C V b ，進行一枚狀跡則跳至步驟 S 113 。

514843

A7  
B7

## 五、發明說明（<sup>148</sup>）

再生器暗語處理部 302 之內部記憶體 307 的系統等名  
稱為 Keys 無論是編號，將中間結果以 DES 進行明暗化並  
加以生成。其次，在步驟 S112 中，用以比較生成後之  
核對值 I C V t 及集管（Header）內之 I C V t，進  
行一致後，其集管步驟 S113。

如前面圖 4 中之說明，總核對值 I C V +，係以核對 I C V a，I C V b，各存儲信息區段之核對部之累加的核對值。因此，藉由上述之處理使該生成功能與其並列於其首 (Header) 之後之核對值。

I C V t 進行一致後時，則被判定 I C V a , I C V b 各存儲器區段之存放個全部知更改。

使存儲信息區級形成為統一對象時，則在步驟 1-14 中，將該區之存儲信息區域，使用記錄再生率 300 處理並 304 取出底層 500 處理，或使用記錄再生率 300 在步驟 305 中由記錄再生率 600 進行接收，並送回至記錄再生率 300 之記錄再生率並處理部 302，將此接收後之記錄再生率並處理部 302 之記錄率 305。係在記錄再生率並處理部 302 之地址／譯碼化部 308 後復存儲信息對象 C 1-15 進行計算。

存儲信息核對值  $I C V i$ ，係如前面說明使區段被準化後時，以存儲信息錄匙  $K e o n$ ，將被輸入後之存儲信息區段以  $D E S$  之  $C B C$  模式進行準化。並將其結果以 8 位元單位進行逐位邏輯和溝通後存之存儲信息中間值以被容納於記錄再生器  $3 0 0$  之內部記憶體 307 後之存儲

- 手机尺寸遵循中国国家标准 (CNS) A4 规格 (210 x 297 毫米) - 151 -

514843

A3  
B3

## 五、晉明說明(149)

信息核對值生成點 Kiev 進行暗號化並加以生成。又，便  
區段未被暗號化時，則將資料（平常文）全體以 B 組元單  
位輸入於圖 3-6 所示之算盤核對值生成器（D E S -  
C B C - M A C )，將存儲信號核對值生成點 Kiev 作為  
（D E S - C B C - M A C ) 之算盤核對值生成點 Kiev。

其次在步驟 S115 中，記錄再生機器號處理部

302之控制部 3-06，係用以比較循序存儲器與累加器，及在累加器 S102由記憶再生器 300之控制部 3-01接收之存儲器監視區段內之 ICV，並將其結果轉寫至記憶再生器 300之控制部 3-01。將此步操作後由記憶再生器 300之控制部 3-01，係在驗正運行成功時，用以取出下次之驗正對象存儲器監視區段在記憶再生器 300之記憶再生器監視部 3-02被驗正，用以鍛鍊再生之存儲器監視部 3-02之正確性（詳參 5116）。

尚有，步驟 S104、步驟 S109、步驟 S112、步驟 S115 之中其一中，未取得核對包之啟動時即做為錯誤進行下載處理終了。

其次，步驟 S<sub>11</sub>7 中記錄再生器將 300 之記錄再生器啓動成處理部 3 0 2，併以步驟 S<sub>11</sub>8 將所欲複寫之區位存取訊號 Kbit 及存位信息指標 Kcon，在記錄再生器啓動成處理部 3 0 2 之時／譯碼化成 3 0 8，在相互應徵時以邏輯上所有啟動之對話時間地帶 Kset 進行逐一檢查，記錄再生器 3 0 0 之控制部 3 0 1，併以對話時間地帶 Kset 作逻辑複寫之後的檢斷資訊 Kbit 及存位信息指標 Kcon 由記

本机供尺度进尺中英制单位 (CNS)A4 规格 (210 × 297 公厘) - 152 -

514843

83

卷一百一十五 150

五、說明說明( )  
該再生器 3 0 0 之記錄再生器增強處理部 3 0 2 產生，並  
將此等資料通過記錄再生器 3 0 0 之記錄裝置控制器  
3 0 3 便能達到記錄與量 4 0 0 。

其次，步驟 S 118 中，由記錄再生器 300 用以接收發送回來之區段資訊編號 Kbit 及存儲信息編號 Xeon 後之記錄匯集 400。依循接收後之資料在記錄匯集匯集器 401 上之順序／層級化器 406，在相互對應時以達行所有放著之對照時間匙匙 Kset 使進行評核，以保存於記錄匯集匯集器 401 上之內記憶體 405 的記錄依據因有之存儲保險匙匙 Kair 再度使用檢驗，記錄再生器 300 之判斷則 301。係述過記錄再生器 300 之記錄來源並判斷圖 303，由記錄匯集 400 以存儲保險匙匙 Kair 用以濾出再層級化之後之區段資訊編號 Kbit 及存儲信息編號 Xeon，即，以記錄時間匙匙 Xair 進行被檢驗化之區段資訊編號 Kbit 及存儲信息編號 Xeon 之彼此的差異。

其次，步驟 S 1 1 9 中，記錄再生器 3 0 0 之錄製部 3 0 1。係由資料之集管部的處理方針（*Usage Policy*）取出用錄製資訊，使下載之後存儲信息進行判定是否可利用該記錄再生器 3 0 0。該判定，係顯示被設定於局域化標記（*利用錄製資訊*）= 1 時，則使進行下載之後之存儲信息也可利用該記錄再生器 3 0 0。而當設定於局域化標記（*利用錄製資訊*）= 0 時，則使進行下載之後之存儲信息也可利用別的同樣之記錄再生器 3 0 0。判定之結果，在累積化標記（*利用錄製資訊*）= 1 時，則追加其

514843

AJ

二、政治思想 · 151

步驟 S 1 2 0 中，記錄再生器 3 0 0 之抑制劑 3 0 1  
 係將記錄再生器固有之抑制劑值在記錄再生器 3 0 0 之記錄  
 再生器固有抑制劑值或記錄 3 0 2 之進行計算。記錄再生器 3 0 0 有  
 之抑制劑，係如圖 2 5 所示在被保存於記錄再生器等級抑制  
 剤 3 0 2 之內部記錄抑制劑 3 0 7 的記錄再生器固有之抑制  
 劑。記錄再生器固有抑制劑 3 0 7 係將記錄再生器 3 0 0 之抑制  
 劑之記錄再生器固有抑制劑值或記錄 3 0 2 之進行抑制化並加以生成。  
 當計算  
 後之記錄再生器固有之抑制劑值 ICVdev，係取代根據對量  
 $ICV_{dev}$  地址上。

如前面所說，系統註冊名稱是 Keys，供在記載系統為了  
與上列註冊名或 I-CV 使用之系統註冊名稱是 Keys。又，記  
錄再生器註冊名稱是 Kdev，在各記錄再生器都不同，以記錄再生  
器為主附上要求名 I-CV 使用之記錄再生器註冊名稱是 Keys。  
即，綠山系統註冊名稱是 Keys 被註冊後之後的資料，係藉由具有同  
樣系統註冊名稱是 Keys（記錄再生器）之後對應到成功，即，  
如果註冊對 I-CV 造成一致，所以成為共同可利用，但使用  
記錄再生器註冊名稱是 Kdev 被註冊時，則記錄再生器註冊  
名稱是 Kdev 有別於其記錄再生器之編號，所以使用記錄再生  
器註冊名稱是 Kdev 被註冊後之後的資料，即，名稱後，被註冊  
於記錄再生器之後的資料，係依其他記錄再生器，以供使其  
記錄裝置前欲再生時，使記錄再生器固有之接續對 I-CVdev  
造成不一致，故須把兩頭以造成不能再生。本發明之資料  
儲存於單一位置，係單一位置而能存取，並在其中可立即  
存取單一位置，係單一位置而能存取，並在其中可立即

Digitized by srujanika@gmail.com



A7  
B7五、發明說明（<sup>156</sup>）

步驟 S 4 0 1 之時間，將譯文化部 4 0 6，在相互認取時以進行共有效率的對話時間論點 Kcs 使譯文化，以保存於記錄裝置增強碼處理部 4 0 1 之內部記憶體 4 0 5 而存儲於記錄裝置固有之保存論點 Ktr 使再譯碼化，記錄再生器 3 0 0 之控制部 3 0 1，保證記錄再生器 3 0 0 之記錄裝置增強碼，記錄再生器 3 0 0 之記錄裝置增強碼 Ktr 用以譯出甚其再譯碼化之後記錄資訊論點 Kbit 及存儲論點 Kbit。即，當初，以記錄裝置 Ktr 被增強碼化之後之記錄資訊論點 Kbit 及存儲論點 Kbit 以保證譯碼 Ktr 用以譯出甚其再譯碼化之後之記錄資訊論點 Kbit 及存儲論點 Kbit。

以下之步驟 S 1 1 9 ~ S 1 2 2，係與前述之格式形態 0 ~ 1 ~ 2 同樣以示省略說明。

以上，係格式形態 3 之中之信道資訊資料之下載處理之類似，則該格式形態 3 之下載處理，係與格式形態 2 同樣，不論存儲供信資訊之錄點，各項信息對信之核對處理，所以成爲迅速可處理，若要求者業實等處理適用於資訊傳輸之他式。又，再譯碼記錄點 Ktr 所以保護而確化存儲信息使範圍被局部化，所以比起格式形態 2，形成更高度之安全性。

其次，對於在格式形態 0 ~ 3 各自之記錄再生器 3 0 0 由記錄裝置 4 0 0 之再生過程使用圖 4 2 ~ 4 5 之流程圖並加以說明。

首先，對於格式形態 0 中之存儲信息的再生處理使用圖 4 2 如以說明。

A7  
B7五、發明說明（<sup>157</sup>）

步驟 S 2 0 1，將記錄再生器及記錄裝置間之認証處理多點，根據前面說明之圖 2 0 0 的認証處理流程圖被執行。

使步驟 S 2 0 1 之認証處理進行移了，並使認証標記被認取，則記錄再生器 3 0 0，係在步驟 S 2 0 2 中，由記錄裝置 4 0 0 根據規定之格式所以譯出甚其之無片，並送達至記錄再生器 3 0 0 之記錄再生器增強碼處理部 3 0 2。

其次，步驟 S 2 0 3 中，使記錄再生器增強碼處理部 3 0 2 之控制部 3 0 6，在記錄再生器增強碼處理部 3 0 2 之信號／譯文化部 3 0 8 之後對值 A 進行計算，依對值 A，係與前面說明之圖 2 3 0 示，將被保存於記錄再生器增強碼處理部 3 0 2 之內部記憶體 3 0 7 的核對值 A 生成論點 Kicva 並被輸出，並將識別資訊（Content ID）及成規方針（Usage Policy）算為信息並計算，其次，在步驟 S 2 0 4 中，用以比較預算算後之核對值 A 及被容納於集管（Header）之內核對值：ICVA，進行一級後時則達到步驟 S 2 0 5。

核對值 A、ICVA，係爲了用以驗證識別資訊，處理萬件之更改的核對值，使裝計算後之核對值 A，與被容納於集管（Header）內後之核對值：ICVA 進行一級後時，則被判斷是否於記錄裝置 4 0 0 之後之識別資訊，處理方針無異狀。

其次，步驟 S 2 0 5 中，記錄再生器 3 0 0 之逆向剖面

A7  
B7五、發明說明（<sup>158</sup>）

3 0 1，係由譯出之後之無片以記錄裝置固有之保存論點 Ktr 取出增強碼化之後之區段資訊論點 Kbit 及存儲信息論點 Kcon，並選取記錄再生器 3 0 0 之記錄裝置控制器 3 0 3 之後對值記錄點 4 0 0。

由記錄再生器 3 0 0 將被發送而來之區段資訊論點 Kbit 及存儲信息論點 Kcon 接收後之記錄裝置 4 0 0，將其接收之後之實所存在記錄裝置增強碼處理部 4 0 1 之增強碼／譯文化部 4 0 8，以保存於記錄裝置增強碼處理部 4 0 1 之內部記錄裝置固有之保存論點 Ktr 使增強碼化處理，若則互認時以進行所有放著的對話時間論點 Kcs 使再譯碼化，該處理，係存在前述之（9）相互認証法之論此交換過程的樣之詳細說明。

步驟 S 2 0 6，係記錄再生器 3 0 0 之控制部 3 0 1，通過記錄再生器 3 0 0 之記錄裝置控制器 3 0 3，由記錄裝置 4 0 0 以對話時間論點 Kcs 用以擷取甚其再譯碼化之後之區段資訊論點 Kbit 及存儲信息論點 Kcon 發送到記錄再生器 3 0 0 之記錄再生器增強碼處理部 3 0 2，並以對話時間論點 Kcs 用以擷取甚其再譯碼化之後之區段資訊論點 Kbit 及存儲信息論點 Kcon 的記錄再生器 3 0 0 之記錄再生器增強碼處理部 3 0 2，係在記錄再生器 3 0 0 之記錄裝置增強碼處理部 3 0 2 之控制點／譯文化部 3 0 8，以對話時間論點 Kcs 被被增強化之

A7  
B7五、發明說明（<sup>159</sup>）

區段資訊論點 Kbit 及存儲信息論點 Kcon，在相互認取時以進行共有效率的對話時間論點 Kcs 使譯文化。

進而，步驟 S 2 0 8 中，以譯文化之後之區段資訊論點 Kbit，在步驟 S 2 0 2 用以譯文化進行派出放著之區段資訊。尚有，記錄再生器 3 0 0 之記錄再生器增強碼處理部 3 0 2，將記錄裝置增強碼處理部 4 0 1 之內部記憶體 3 0 7 的核對值 Kcon 及區段資訊論點 Kbit，存儲信息論點 Kcon 及區段資訊論點 Kbit，在步驟 S 2 0 2 重複被合於派去之後之無片的存儲資訊論點 Kbit，存儲信息論點 Kcon 及區段資訊論點 B IT，並將記錄裝置增強碼處理部 3 0 1，係將被辨識化之後之區段資訊論點 Kbit 由記錄再生器 3 0 0 之記錄再生器增強碼處理部 3 0 2 送出放著。

進而，在步驟 S 2 0 9 中，記錄再生器增強碼處理部 3 0 2 之控制部 3 0 6，係由基底資訊論點 Kbit，存儲信息論點 Kcon 及區段資訊論點 B IT，而以生成核對值 B（ICVB），核對值 B，係與圖 2 4 0 所示，將被保存於記錄再生器增強碼處理部 3 0 2 之內部記憶體 3 0 7 的核對值 B 及論點 Kcon 故為論點，將由區段資訊論點 Kbit，存儲信息論點 Kcon 及區段資訊論點 B IT 所構成之數字邏輯和以 D E S 進行階級化並加以生成，其次，在步驟 S 2 1 0 中，所以被核對值 B 及集管（Header）之 ICVB，進行一級後時達到步驟 S 2 1 1。

核對值 B、ICVB，係爲了用以驗證區段資訊論點 Kbit，存儲信息論點 Kcon，區段資訊論點 B 之修改的核對值，便生成之後之核對值 B，與被容納於集管（Header）之核對

A7  
B7

## 五、發明說明 (160)

值「ICV b」進行一致後時，係被判斷是否保持於記錄裝置 4 0 0 後之資料中之區存資訊編號 Kbit，各存儲信息編號 Econ，區存資訊數量。

步驟 S 2 1 1 中，記錄再生器識號處理部 3 0 2 之註冊部 3 0 5，係在記錄再生器識號處理部 3 0 2 之倍數 / 語音化部 3 0 8 使中間核對值以計算，中間核對值，係如圖 2 5 所示，將被保存於記錄再生器識號處理部 3 0 2 之內部記錄體 3 0 7 的規範對應至底端地址 Kiev，係為地址，並將該底端之後之 Header 對應值 A，核對值 B，並按資訊中之空隙存儲信息核對後做為信息項並以圖 7 其核對規範之 ICV 計算方法進行計算，向右，生成並之中間核對值，係根據必要保持於記錄再生器 3 0 0 之記錄再生器識號處理部 3 0 2 故步。

其次，步驟 S 2 1 2 中，記錄再生器 3 0 0 之控制部 3 0 1，係由記錄裝置 4 0 0 之外記錄裝置 4 0 2 被合於之後之資料的蓄管部由底端地址為「Usage Policy」取出用限制資訊，使再生器定之存儲信息進行判斷並可利用該記錄再生器 3 0 0 (利用限制資訊為 1)，或也可利用別之規範之記錄再生器 3 0 0 (利用限制資訊為 0)。判定之結果，利用限制資訊為 1，即，使再生器僅僅僅可利用該記錄再生器 3 0 0 之設定並使用限制，逕到步驟 S 2 1 3，而利用限制資訊為 0，其也可利用別的同樣之記錄再生器 3 0 0 後定時，則逕到步驟 S 2 1 5。尚有，步驟 S 2 1 2 之處理係進行記錄再生器識號處理部 3 0 2

本辦法適用於中國國家標準 (CNGB/AH 號令 (200+207 公司) - 163 -

A7  
B7

## 五、發明說明 (161)

也可。

步驟 S 2 1 3，係記錄再生器 3 0 0 之底部部 3 0 1，係記錄再生器識號由其核對值 ICVdev 在記錄再生器 3 0 0 之記錄再生器識號處理部 3 0 2 進行計算，記錄再生器識號由其核對值 ICVdev，係如圖 2 5 所示，將被保存於記錄再生器識號處理部 3 0 2 之內部記錄體 3 0 7 的記錄再生器識號 Kdev 為輸出，並在步驟 S 2 1 1 將進行保存於該的中間核對值以 DES 進行密鑑化加以生成。

其次，步驟 S 2 1 4 中，在步驟 S 2 1 3 用以比較進行計算之後之記錄再生器識號由其核對值 ICVdev 及在步驟 S 2 0 2 進行運出之後之無管內之 ICVdev，並在有一致後時，逕到步驟 S 2 1 7。

另外在步驟 S 2 1 5，係記錄再生器識號處理部 3 0 2 之語音化部 3 0 6，係在記錄再生器識號處理部 3 0 2 之倍數 / 語音化部 3 0 8 使中間核對值 ICV t 進行計算，總核對值 ICV t，係如圖 2 5 所示，將被保存於記錄再生器識號處理部 3 0 2 之內部記錄體 3 0 7 的系統名稱碼 Keys 為輸出，將中間核對值以 DES 進行密鑑化並加以生成。其次，步驟 S 2 1 6 中，用以比較生成之後之核對值 ICV t 及無管 (Header) 之內之 ICV t，在進行一致後時，則逕到步驟 S 2 1 7。

總核對值 ICV t，及記錄再生器識號由其核對值 ICVdev，係為了用以驗證 ICV a，ICV b 各存儲信息區段之核對值全部之寫成的核對值。因此，藉由上述之威

本辦法適用於中國國家標準 (CNGB/AH 號令 (200+207 公司) - 164 -

A7  
B7

## 五、發明說明 (162)

理被生成之後之核對值被寄存於無管 (Header) 內後之核對值：ICV 1 或 ICVdev 在進行一致後時，係被判斷被寄存於記錄裝置 4 0 0 後之 ICV a，ICV b，各存儲信息區段是否之核對值全部為無數。

接著，步驟 S 2 1 7 中，記錄再生器 3 0 0 之控制部 3 0 1，係由記錄裝置 4 0 0 以導出底端資料，進而，步驟 S 2 1 8 中用以判定是否密鑑化，被密鑑化時，則記錄再生器 3 0 0 之記錄再生器識號由其核對值處理部 3 0 2 中進行存取資料之拆解，並被密鑑化時，則跳過步驟 S 2 1 9 並逕到步驟 S 2 2 0。

其次，步驟 S 2 2 0 中，記錄再生器 3 0 0 之控制部 3 0 1，係根據區段資訊 (B I T) 內之存儲信息區段資訊，調查存儲信息區段是否為成員對象，使存儲信息區段成為點對點對象時，在當集中之區段資訊中使存儲信息核對對象資訊，使存儲信息區段成為高級對象後時，則在步驟 S 2 2 1 中，使該當之存儲信息區段之存儲信息核對值 ICV 1 進行計算，使存儲信息區段成為點對對象時，則跳過步驟 S 2 2 1 及步驟 S 2 2 2 並逕到步驟 S 2 2 3。

存儲信息核對值 ICV 1，係如前述圖 3 6 之說明甚麼被密鑑化時，以存儲信息編號 Econ，將被輸入後之存儲信息區段以 DES 之 C B C 模式進行密鑑化，將其結果全部以 8 位元單位進行排他性聯繫和其生成後之存儲信息中間值以密鑑於於記錄再生器 3 0 0 之內部記錄體。

A7  
B7

## 五、發明說明 (163)

3 0 7 後之存儲信息核對值生成編號 Kievc 進行密鑑化並加以生成。又，當發送密鑑化時，則將資料 (平常文) 數據以 8 位元單位進行輸入於圖 3 6 所示計算機對值生成函數 (DES-C B C-MAC)，將存儲信息核對值生成編號 Kievc 作為傳輸 (Header) 故而取得傳輸生成。

步驟 S 2 2 2 中，記錄再生器帶狀處理部 3 0 2 之控制部 3 0 3，係用以比較生成之後之存儲信息核對值 ICV 1，及在步驟 S 2 0 2 由記錄再生器 3 0 0 之控制部 3 0 1 將其結果進行接收後之記錄再生器 3 0 0 之控制部 3 0 1，將此進行接收後之記錄再生器 3 0 0 之控制部 3 0 1，係在驗正進行成功後時，在步驟 S 2 2 3 中，在記錄再生器系統 R A M 上以讀新執行 (再生) 用存儲組合平常文資料，記錄再生器 3 0 0 之控制部 3 0 1，係並用以取出下次之驗正對象存儲信息區段並在記錄再生器 3 0 0 之記錄再生器識號處理部 3 0 2 使進行驗正，將全部之存儲信息區段進行驗正為存儲回憶之驗正函數，R A M 索納處理 (步驟 S 2 2 4)。

尚有，在步驟 S 2 0 4，步驟 S 2 1 0，步驟 S 2 1 4，步驟 S 2 2 2 中，步驟 S 2 2 2 之中之一，未取得核對值之一致時則做為錯誤並終了再生處理。

步驟 S 2 2 4 中被判定主存段被指出，則逕到步驟 S 2 2 5，使存儲信息 (程式，資料) 之執行，再生被開始。

本辦法適用於中國國家標準 (CNGB/AH 號令 (200+207 公司) - 165 -

本辦法適用於中國國家標準 (CNGB/AH 號令 (200+207 公司) - 166 -



## 五、發明說明 (168)

啟動的對話時間範圍 Ktes 使進行詳情化。

然而，步驟 S 2 0 8 中，以詳情化後之區段資訊編址 Kbit，在步驟 S 2 0 2 用以詳情化進行讓出後的區段資訊，尚有，記錄再生器 3 0 0 之記錄再生器和地址處理部 3 0 2，係將詳情化後之新段資訊編址 Kbit 及區段資訊 B I T，在步驟 S 2 0 2 實施或結合讓出後之單管的區段資訊編址 Kbit 及區段資訊 B I T 並進行保存狀態。又，記錄再生器 3 0 0 之控制部 3 0 1，係將詳情化後之區段資訊編址 Kbit 由記錄再生器 3 0 0 之記錄再生器號碼識別部 3 0 2 處理出放送。

然而，步驟 S 2 5 4 中，記錄再生器組合處理部 3 0 2 之控制部 3 0 6，係由該段資訊編址 Kbit 及區段資訊 ( B I T )，用以生成對值 ( I C V b )。核對值 3，係如圖 2 4 所示，將該再生器記錄再生器單管號碼處理部 3 0 2 之內部記憶體 3 0 7 的樣對值 B 生成對值 Kicvb 作為識別，藉由該資訊編址 Kbit 及區段資訊 ( B I T ) 所構成之單管狀態和以 D E S 行進單管化並以此生成。其次，參照 S 2 1 0 中，可以比較對值 B 及標題 ( Header ) 內之 I C V b，在進行一致後即進到步驟 S 2 1 1。

若式形態 3，係道，由該級編址記錄裝置在查詢時未存儲此因為被確認為，所以在記憶裝置 4 0 0 中以存取速度之擇而為處理，以及以對稱開關點之確認為是，進而，在記錄再生器 3 0 0 以對稱開關點此之詳情化為必要，據此等之一連串的處理在步驟 S 2 5 5，步驟

## 五、發明說明 (170)

生產過程被執行，使步驟 S 2 1 7 ~ 步驟 S 2 4 3 之處理對於全區段進行重複被執行。步驟 S 2 4 4 中被判定全區段讓出進行終了再生處理。

以上之處理，係依式形態 3 中之存儲信息的再生處理，在欲存取總對值之效應處理之點兩式形態 2 款類似，但不會因級編址之輸送交換處理之點比階級式形態 2，進而形成高安全性的水平之兩端結構。

( 1.1 ) 存儲信息提供者中之核對值 ( I C V ) 生成處理機制

在上述實驗例中，使對於各種狀對值 I C V 之被認處理，在存儲他倉之下載，或再生處理之時被兩次執行之事加以說明。於此，係對於各級對值 ( I C V ) 生成處理，核對值之效應加以說明。

首先，對於實施例說明之各級對值，以兩個來舉，則本發明之資料處理裝置中被利用之核對值 I C V 係有以下之核對值。

核對值 A 、 I C V a：爲了用以驗證該個信息資料中之識別資訊 ( Content ID ) 、處理方針 ( Usage Policy ) 之更改的核對值。

核對值 b 、 I C V b：爲了用以驗證該個信息資料中之存儲信息編址 Kcon 之更改的核對值。

存儲信息核對值 I C V c：爲了用以驗證核對值 I C V a 、核對值 I C V b 、各存儲信息區段之核對值全

## 五、發明說明 (169)

S 2 5 6 被顯示之處理步驟。

在步驟 S 2 5 5，記錄再生器 3 0 0 之控制部 3 0 1 係在步驟 S 2 1 7 由讓出後之區段以記錄復原面有之保存識別 Ktr 用以取消單管化後之區段轉其 Kbit，並進而記錄再生器 3 0 0 之記錄資訊單管削器 3 0 3 使後到記錄裝置 4 0 0 。

由記錄再生器 3 0 0 用以接收單管回來之區段轉其 Kbit 的記錄復原 4 0 0 ，係將所接收之後之資料在記錄復原面號處理部 4 0 1 或接續 / 詳情化部 4 0 6 ，以保存於記錄復原面號處理部 4 0 1 之內部記憶體 4 0 5 的記錄裝置固有之保存識別 Ktr 使進行詳情化處理，在相互認定時以進行共有放送的對話時間範圍 Ktes 使進行再階級化，該處理，係知前述之 ( 9 ) 在相互認定後之縮影交換或處理，便已能詳細說明。

步驟 S 2 5 6，係記錄再生器 3 0 0 之控制部 3 0 1 係將所接收記錄再生器 3 0 0 之記錄資訊單管削器 3 0 3 ，由記錄裝置 4 0 0 以對話時間範圍 Ktes 用以接收被再階級化後之區段轉其 Kbit 。

其次，步驟 S 2 5 7 中藉由記錄再生器 3 0 0 之記錄資訊單管削器 3 0 3 之對話時間範圍 Ktes 之對話時間範起 Ktes 之再階級化處理。

其次，步驟 S 2 4 2 中，在步驟 S 2 5 7 使用被詳情化之後之區段轉其 Kbit 。

步驟 S 2 4 3 中，使用存儲信息 ( 程式、資料 ) 之執行，再

## 五、發明說明 (171)

述之變改的核對值。

記錄再生器團圓之核對值 ( ICvdev )：使用內部標記號設定期於 1 時，即，是否備信息顯示可利用於記錄再生器團圓時，可選擇或總核對值 I C V t 之核對值 A : I C V a 、核對值 B : I C V b ，進而對於該倉於形成存儲信息之核對值對象的各區段之核對值 I C V 之全體做為該對值被生成。

藉由格式，即 I C V t 、 ICvdev 被結合於核對之對象，係並非存儲信息團圓之核對值，也有形成存儲信息核對值之情形。

以上之各核對值係被使用在本發明之資料處理裝置中，在上述各種對值之中，核對值 A ，核對值 B ，總核對值存儲信息團圓時，係譬如被顯示於圖 3 2 ~ 3 5 ，及圖 6 用以提供存儲信息資料之存儲信息團圓使 I C V 值被生成，與存儲信息一起被容納於資料中並提供給記錄再生器 3 0 0 之利用者，記錄再生器之利用者，即存儲信息使用者，存儲信息團圓是在記錄資訊單管進行下載時，或進行再生時分別根據該對值對象資料用以生成驗證用之 I C V ，並與許容之 I C V 值進行比較，又，記錄再生器團圓有顯示有之核對值 ICvdev ，係將存儲信息在記錄再生器團圓用顯示時，可識別該對值對值 I C V t ，並被容納於記錄裝置。

核對值之生成處理，係在前述之實驗例中，係主要藉由 D E S - C B C 用以說明生成過程構成。可是，在 I C V

## 五、發明說明 (172)

生成或處理應像，係不限定於上述方法有種種的生成處理應像，而有兩種種的証據或應像者，特別是存儲信息提供者或管理者，及存儲信息利用者之關係中，可有以下說明之名稱：I C V 生成或應像處理構成。

圖 4-6 ~ 圖 4-8 係顯示核對該 I C V 之生成者中之生成處理，及藉由驗證者用以說明驗證處理圖。

圖 4-6 係在上述之實體剖面圖由說明之 D E S - C B C 沿 I C V 之生成處理，譬如以存儲信息提供者或管理者進行 I C V 生成者，將生成後之 I C V 與存儲信息一起提供到記錄再生器利用者，即提供給驗證者之據成，該情形使記錄再生器利用者，即驗證者在驗證時成為必要驗證者，係將其被容納於圖 1-8 所示紀錄器體 307 後之各核對對應生成處理利用者之據成（記錄再生器利用者），併使用被容納於內部記錄體 307 後之核對面對應生成器對應生成以執行此據成者，該情形，各核對產生此據成，並述標成與 I C V 之生成者，配馳驗證者做為共同有之據成。

圖 4-7 係使存儲信息提供者或管理者之 I C V 的生成者藉由公開編址號系統之數位署名用以生成 I C V，將生成後之 I C V 與存儲信息一起提供到存儲信息利用者，即驗證者，存儲信息利用者，即驗證者，係用以保存 I C V 生成者之公開編址，並使用該公開編址用以執行 I C V 之驗證處理的構成。該情形，存儲信息利用者（記

## 五、發明說明 (174)

對於根據主導者之各據成被認為適用據成的生成構成加以說明。

使用如前圖圖 1-8 之說明，在本發明之資料處理與實體中心之記錄再生器 300 的內部記錄體，保謄種種的主導者之據成，使用此等之各主導者，譬如形成用以生成（參考款 3）記錄號 Kite，應用以生成（參考款 4）配馳號 Kite 等構成。

首先，1 對 1 之實體從，即存儲信息提供者及存儲信息利用者兩者，或，在上邊之本發明的資料處理裝置中之記錄再生器 300 及記錄再生器等之進行追號資訊，相互通報，M A C 成，驗證者，係在名實體間保持共同的密碼資訊，譬如使保持有繪字資訊。又，1 對多之關係，實例 1 個之記錄再生器對多數之存儲信息利用者，或 1 個之記錄再生器對多數之記錄號等之事件中，全部之實體，用多數之存儲信息利用者，或多數之記錄號等中使共有之密碼資訊，譬如使據此資訊而保持據成構成，或，便 1 個之存儲信息提供者以分別用以管理多數之存儲信息利用者各自之秘密資訊（e x . 鑰匙），並若此據存儲信息利用者分開使用。

可見，如上述有 1 對多之利用據成商，則使全部用以所有與之秘密資訊（e x . 鑰匙）的構成中，僅僅生 1 之祕密改編新利用同個資訊者會全部受到影響之缺點。又，1 個之管理者，譬如及多數個信息提供者以個別用以管理多數之存儲信息利用者各自之秘密資訊（e x . 鑰

## 五、發明說明 (173)

再生器或利用者），即驗證者具有之 I C V 生成者的公私鑰匙係不必保密，當僅僅作為容易，且 I C V 之生成，實理在 1 個實體中被執行時等，使 I C V 之生成，管理適合以高安全性管理水準並進行良好的性質。

圖 4-8 係使存儲信息提供者或管理者之 I C V 的生成者藉由公開編址號系統之數位署名用以生成 I C V，將生成後之 I C V 與存儲信息一起提供到存儲信息利用者，即驗證者，進而，使驗證者使用驗證者公開證明書（參見參考圖 1-4）與存儲信息實質一和提供到記錄再生器利用者，即驗證者，使 I C V 之生成者或據成存在時，各生成者，併應用以證明公開編址號此之正確性的資料（公開編址證明書）在論證管理中心進行作成。

I C V 之驗證者的存儲信息利用者，係將其據成管理中心之公開編址，驗證者將將公開編址證明書之驗證藉由驗證管理中心執行，使正確性被確認的話，用以取出被啟動於該公開編址證明書之 I C V 之生成者的公開編址。而且，使用取出後之 I C V 的生成者之公開編址用以執行 I C V 之驗證。

該方法，係依 I C V 之生成者為準，藉由而以執行此等之管理的中心據成管理之執行系統往進行確立時得有效之應變。

## (1)2 根據主導者之帶號處理據成構成

其次，本發明之資料處理系統中之特徵性的構成之一

## 五、發明說明 (175)

此，將此根據各據成信息利用者分開用以做為構成，則用以識別全部之利用者，且在此據成資訊（e x . 鑰匙）的名單，讓各利用者之增大會增加名單之據成管理負擔的缺點。

本發明之資料處理裝置中，在如此之實體間將秘密資訊其有之共用的開始由主導者之保有，及由主導者藉由用以生成各種之個別據成的構成或進行解決，以下對於據成加以說明。

本發明之資料處理裝置中，係用以發送紀錄號或存儲信息之據成，或在記錄再生器間從各據成之據成處理，認證處理等中之不與個別的據成形成必要時，將其個別之據成，使據成或據成之因有保護據成子資訊（I D ）等在個別資訊及紀錄再生器 300 內使用預先被決定之個別據成生成方式進行生成，藉由該構成為一，使被生成者之個別據成被確定也就能止主導者之洩漏，則據成可防止對系統全體的被害。又藉由主導者根據用以生成據成之據成也成為不對對應者之管理。

對於具體之據成例，使用圖加以說明。首先，圖 4-9 係顯示將各據成使用記錄再生器 300 具有之各據成主導者形以說明生成或據成圖，由圖 4-9 之機體 500、通訊裝置 700、係與已經說明之實施例同様，使存儲信息被存儲，存儲信息保護由存儲信息編址 Kon 被稱號化，又，存儲信息據成 Kcos，係將由配馳號 Kds 被稱號化。

譬如，使記錄再生器 300 由機體 500、憑証裝置

## 五、發明說明 (176)

6 0 0 用以取出存儲信息，在記錄裝置 4 0 0 次進行下載時，若於步驟 2 2 ，圖 3 9 ~ 4 1 之說明，記錄再生器 3 0 0 程，或形或必將存儲信息轉換進行編號化用以取得記錄裝置 Kdis · 記錄逆轉點 Kdis 由媒體 5 0 0 ，資訊裝置 6 0 0 直接取得，或預先使記錄再生器 3 0 0 並行取得也可容許記錄再生器 3 0 0 內之操作者，但對如此操作之多數的使用者之配布構成，係如前面也說明在系統全體有可能受到改變之影響。

本發明之資料製造系統，其構成具有，將該記錄裝置 Kdis 如顯示於圖 4 9 之下部，被容納於記錄再生器 3 0 0 之記憶體內的記錄裝置 Kdis 由主機 MKdis ，及根據存儲信息 I D 之生成，即通過 Kdis = D E S ( M Kdis 、存儲信息 I D ) 用以生成記錄點 Kdis · 然依據本構成，則由媒體 5 0 0 · 資訊裝置 6 0 0 用以供給存儲信息之存儲信息提供者及在該存儲信息利用者的記錄再生器 3 0 0 間之存儲信息之傳輸構成中，從存儲信息提供者使步驟存儲時，也不必將存儲之記錄裝置 Kdis 透過該點，資訊該點使資訊又，也不必要容納於各記錄再生器 3 0 0 ，形成可保持高度安全性。

其次，對於記錄輪點 Kdis 之生成加以說明，由前面已說明於圖 2 2 ，圖 3 9 ~ 4 1 之記錄再生器 3 0 0 記錄裝置 4 0 0 下載或寫，並將被容納於步驟 2 8 ，圖 4 2 ~ 4 5 指向之記錄裝置 4 0 0 後之存儲信息在記錄再生器 3 0 0 中進行執行，再生時，即將被容納於圖 2 8 ，圖 4 2 ~ 4 5 指向之記錄裝置 4 0 0 後之存儲信息在記錄再生器 3 0 0 中進行執行，再生時，形成有必要在記錄再生器

本技術文字適用中國專利標準(CNSA)規格(GB/T 207 公里) - 179 -

## 五、發明說明 (178)

根據必要如圖 4 9 之下部所示記錄再生器點子： I D dev 及根據記錄再生器名稱點用主機點 Kdev ，理由 I D dev = D E S ( M Kdev , I D dev ) 故而求出記錄再生器名稱點 Kdev ，無必要使記錄再生器都有名稱點 Kdev 保持於機器側使之點點。

如此，本發明之資料製造系統中，如提供者及記錄再生器，或記錄再生器及記錄裝置間之 2 個實體間在有解說資訊與處理的手段所必需之點點等的資訊由主機及名 I D 依循逐漸進行生成之傳成，所以使這些資訊由名實體即記錄點產生之傳成，但藉由個別點點之資訊範圍而被限定，又如於這些個別實體也形成不重複點名之問題。

對於有質本構成之後數處理用以顯示流程加以說明，圖 5 0 0 用以存儲信息製作管理者中之主機此之存儲信息等之傳號化處理，及使用者與質，譬如上述之實例例中之記錄再生器 3 0 0 中用以主機點之傳號化資料的傳送處理，

存儲信息製作或管理者中之步驟 S 5 0 1 ，係對存儲信息指派別于之步驟，步驟 S 5 0 2 ，添置存儲信息製作或管理者具有之主機點及存儲信息 I D 與存儲信息等之傳號化用以生成記錄點 Kdis 之步驟，此係將如，若欲為用以生成記錄點 Kdis 之工程，則藉由前述之 Kdis = D E S ( M Kdis , 存儲信息 I D ) 用以生成記錄點 Kdis 。其次，步驟 S 5 0 3 ，係將存儲信息之一部分，或全部藉由點點(譬如記錄點 Kdis )進行傳號化之步驟，存儲信息製作

本技術文字適用中國專利標準(CNSA)規格(GB/T 207 公里) - 181 -

## 五、發明說明 (177)

3 0 0 及記錄裝置 4 0 0 間之記錄再生器 3 0 0 (參考圖 2 0 )。

如圖 2 0 之說明，該認證傳播中之記錄再生器 3 0 0 係有必要形成記錄點 Kdis · 記錄再生器 3 0 0 ，倘若認證傳播始由記錄裝置 4 0 0 直接取得，或預先使記錄再生器 3 0 0 進行取值也可容納於記錄再生器 3 0 0 內之記錄點放棄，但將上之記錄點構成之構成同樣，但對如此論點之多數的使用者之配布構成，在系統全體有可能受到改變之影響。

本發明之資料製造系統，其構成係具有，將該記錄點 Kdis 如顯示於圖 4 9 之下部，並容納於記錄再生器 3 0 0 之記憶體內的記錄點 Kdis 由主機點 M kdis ，及根據記錄點 I D 證明 I D ，圖 2 0 認證，那樣由 Kdis = D E S ( M kdis , I D m ) 之出認證點 Kdis 。

而後，由圖 2 2 ，圖 3 9 ~ 4 1 之記錄再生器 3 0 0 對記錄裝置 4 0 0 之下載或寫，並將被容納於步驟 2 8 ，圖 4 2 ~ 4 5 指向之記錄裝置 4 0 0 的存儲信息在記錄再生器 3 0 0 中進行執行，再生時，在可利用於記錄再生器 3 0 0 有之存儲信息是在記錄再生器點子之記錄點 I C D v d s 之生成或為必要對於記錄再生器帶名稱點 Kdev 也可做與上之記錄點構成，該認證點此同樣的構成，在此之實例例中，可稱參見後再生器帶名稱點 Kdev 係做為客納於內部記錄點之構成，因該記錄再生器帶名稱點用主機點 M kdis 容納於記錄點，而記錄再生器帶名稱點 Kdev 係不導於記錄點，

本技術文字適用中國專利標準(CNSA)規格(GB/T 207 公里) - 180 -

## 五、發明說明 (179)

者，係由於如此之步驟將進行傳號化處理後之存儲信息通過 D V D 等之媒體，資訊擴廣等並進行配訛。

另外，實質在記錄再生器 3 0 0 等之利用者皆僅僅，係在步驟 S 5 0 4 中，透過媒體，資訊擴廣等由接受後之存儲信息實質用以取出存儲信息 I D 。其次，步驟 S 5 0 5 中，將認證出之之存儲信息 I D 及所有之主機此用以生成應用於傳號化存儲信息之詳列的點點。該此生成或寫，或將存儲點記錄點 Kdis 之處理時，則當如形成記錄點 Kdis = D E S ( M kdis , 存儲信息 I D ) 。在步驟 S 5 0 6 ，使存儲信息用以識讀存儲信息，並在步驟 S 5 0 7 運用記錄存儲信息，即用以執行再生或程式。

請例中，係如圖 5 0 0 下段所示，存儲信息製作或管理者，及使用用於存儲之雙方具有之主機點(譬如記錄點再生用主機點 M kdis )，在存儲信息之傳號化，釋放將必要的記錄點分別識別並進行所有之主機此指各 I D (存儲信息 I D )加以生成。

該系統，係萬一使記錄點起點指給第三者時，使該存儲信息之傳兩不同能底放在第三者，但為了可用以防止存儲信息 I D 之不同其他的存儲信息之傳播，可具有使 1 個之在存儲信息點子的改善將影響到系統全體為着小幅度的效果。又，利用者要點，即記錄再生器中，亦具有不必要以保存存儲信息點子之用而簡單的效用。

接著使用於 S 5 1 ，對於後存儲信息製作或管理者用以所有模數之主機點，並用以執行依據存儲信息之記錄對象

本技術文字適用中國專利標準(CNSA)規格(GB/T 207 公里) - 182 -

五、發明說明<sup>(180)</sup>  
的處理則以說明。

存儲信息製作或管理者中之步驟 S 5 1 1，係對存儲信息賦予識別碼子（存儲信息 ID）之步驟。步驟 S 5 1 2，係由存儲信息製作或管理者具有之主論此（譬如說其之配達地點生成用主論此 MKdis）所以選擇 1 個之主論此的步驟。該選擇處理係使用圖 5-2 來藉以說明，但附註的是存儲信息之利用者的各國、各種種類、或機種類或等將先用以設定選出之主論此放著，依據該設定進行執行主論此。

其次，在步驟 S 5 1 3，係根據在步驟 S 5 1 2 選擇後之主論此，及在步驟 S 5 1 1 決定設之存儲信息 ID 用以生成識別號化用之識別號。此係當初，若使應用以生成配達地點 Kdis 之工程，則系由 Kdis = Kdis 1 (MKdis, 存儲信息 ID) 以生成。其次，步驟 S 5 1 4 係將存儲信息之一部分，或全部藉由識別號（譬如配達地點 Kdis）進行識別化之步驟。存儲信息製作者，若在步驟 S 5 1 5 中，若將存儲信息 ID，使用後之主論此將變異時，及時變化存儲信息係依 1 個之配布單位將該行號化處理之後之存儲信息道過由 DVD 之媒體，道過裝置等進行配記。

另外，譬如在記錄再生器 3 0 0 等之利用者装置，步驟 S 5 1 6 中，通過 DVD 等之媒體、訊送裝置等將對應於該訊之後之存儲信息資料中的主論此識別資訊之主論此對於是否自己所有加以判定。未持有對應於存儲信息資料中之主論此識別資訊的主論此時，則其配布存儲信息

五、發明說明<sup>(181)</sup>  
，係在其利用者裝置中不能應用，並終了處理。

對應於前述訊之後之存儲信息資料中的主論此識別資訊之主論此係依自己所有時，則在步驟 S 5 1 7 中，透過裝置、訊送裝置等由接受後之存儲信息資料中以譯出存儲信息 ID。其次，在步驟 S 5 1 8 中，根據譯出之後之存儲信息 ID 及所有之主論此用以生成適用於識別號化存儲信息之辨識，並生成處理，係取憑據逆轉地 Kdisi → Kdisi 之處理時，則會如形如配達地點 Kdisi = D E S (MKdis, 存儲信息 ID)。在步驟 S 5 1 9，係使用該識別號用以存取存儲信息，並在步驟 S 5 2 0 利用譯碼存儲信息，即用以執行再生或程式。

在該例中，係當初 B 1 下設所示，存儲信息製作或管理者，係具有複數之主論此。譬如由複數之配達地點生成用主論此 MKdis 1 ~ n 所構成之主論此組。另外，在利用者裝置係 1 個之主論此譬如若具有 1 個之配達地點生成用主論此 MKdis 1，從存儲信息製作或管理者用 MKdis 1 促進行識別化處理的，而所做裝置，係可利用用以譯碼其存儲信息。

做為該案 S 5 1 所述之流程樣式的具體內容，係將適用各項不同主論此之例顯示於圖 5-2。存儲信息製作者，係具有主論此 MK 1 ~ s，MK 1 係設定有配備於通過日本之利用者裝置用以執行存儲信息之識別號化處理的識別號。譬如，由存儲信息 ID 及 MK 1 用以生成識別號化地點 K 1 並藉由 K 1 用以識別化存儲信息。又，MK 2 係配備

五、發明說明<sup>(182)</sup>

於適合 U 之利潤者若要應用以執行存儲信息之識別號化處理的識別號，而 MK 3 係配備於適合 EU (歐洲) 之利用者裝置用以執行存儲信息之識別號化處理的識別號。

另外，適合日本利用者裝置、具體而言係在日本被販賣之 P C 或遊戲機等之記錄再生器，係使主論此 MK 1 裝置等於其內部記錄盤，在適合 U 之利用者裝置，係使主論此 MK 2 被容納於其內部記錄盤，在適合 EU 利用者裝置，係使主論此 MK 3 被容納於其內部記錄盤。

在此之構成中，存儲信息提供者，係將存儲信息提供可利用之利用者裝置，以選擇地點 K 1 用以選擇地點 K 1 用以執行配記於利用者裝置之存儲信息的識別號化處理，譬如所存儲信息為了做某項可用以適合日本之利用者裝置，係使用主論此 MK 1 之主論此生成後之主論此 K 1 用以識別化存儲信息。該識別化存儲信息，係使用該存儲信息適合日本利用者裝置之後之主論此 MK 1 可譯得，即可生成識別號化地點，但由選擇地點 K 1 用以適合日本之利用者裝置之主論此 MK 2、MK 3 係不能取得地點 K 1，所以形成不可能識別化存儲信息之識別號。

如此，使存儲信息提供者藉由選擇性使用複數之主論此，可表示以設定種種之存儲信息的利用限制。圖 5-2 係顯示在利用者裝置之圖別用以區分主論此之例，例如前述，衣架利用者裝置之後，或根據基式可切換主論此等，可獲得利用形態。

其次，圖 5-3 係顯示幾個有之識別號子，即將識別

五、發明說明<sup>(183)</sup>

ID 及主論此組合之處理例。於此，所謂兩種係指扣用以零的 DVD、CD 等之存儲信息之後之媒體，媒體 ID，係在 1 個 1 個之各媒體裏面固有也可，譬如，在電影等之存儲信息各媒體固有也可，並在媒體之各製造批號做為固有也可。如此做為媒體 ID 之分派方法可使用種種的方法。

存儲信息製作或管理者中之步驟 S 5 2 1，係對識別用以決定製劑子（媒體 ID）之步驟。步驟 S 5 2 2，係根據存儲信息製作或管理者具有之主論此及媒體 ID 用以生成將媒體之各媒體內存儲信息等進行識別化地點的步驟。此係當初，若當初用以生成配達地點 Kdis 之工程，則應由前述之 Kdis = (MKdis, 認識 ID) 用以生成配達地點 Kdis。其次，步驟 S 5 2 3，係將其媒體內容存儲信息之一部分，或全部藉由識別號（譬如配達地點 Kdis）進行識別化之步驟。媒體製作者，係經由如此之步驟用以供給進行識別化處理之後之存儲信息的媒體。

另外，譬如在記錄再生器 3 0 0 等之利用者裝置，係在步驟 S 5 2 4 中，由被供給後之媒體用以譯出媒體 ID。其次，在步驟 S 5 2 5 中，根據譯出之後之媒體 ID 及所有之主論此用以生成適用於識別化存儲信息之識別號。該識別號，係生成處理，係取得配達地點 Kdisi 之處理時，則會如形如配達地點 Kdisi = D E S (MKdis, 媒體 ID)。在步驟 S 5 2 6，係使用該識別號用以譯碼存儲信息，並在步驟 S 5 2 7 利用譯碼存儲信息，即用以執行再生或程式。

AF  
BT

## 五、發明說明（184）

在該例中，如圖 5-3 下段所示，媒體製作或管理者、及美利亞者設置之雙方具有主導點（譬如配送施加生成用主導點 MKdis），在存儲信息之暗化、譯碼所必要的配送施加分別逐行所有之主導點根據各 ID（媒體 ID）加以生成。

該系統，係萬一使媒體施加相應於第三步時，使該媒體內存儲信息之譯碼可參考或依循第三步，但為了可用以防止被密約的媒體 ID 之不同其他媒體後之存儲信息的譯碼，其具有使 1 倍之媒體識別的長度將影響到系統全體做為最小限度的效果。又，使用者若要觀閱，即記錄再生器中，也真無必要以保持各媒體識別之財別名單的效果。

又，以 1 倍之媒體施加相應於第三步時，係萬一其媒體內為了該限制於可密約之名單，爲了能擴大攻擊達到必要的資訊量可能性很少，所以可蒙單誌該運之可能性減低。

其次，圖 5-4 係顯示記錄再生器有之類別，即將記錄再生器 ID 及主導點組合之範例。

記錄再生器利用者之中步驟 S 5-3-1，係著如根據被密約的記錄再生器之內部記錄保持之主導點及記錄再生器 ID 用以生成存儲信息等進行相應化之輸點的步驟。此步驟之密約，係著用以生成存儲信息譯點 Kcon 之工程，則將由 Kcon = DES (MKcon)、記錄再生器 ID 用以生成存儲信息譯點 Kcon。其次，步驟 S 5-3-2，係將密約存儲信息之部分，或全稱藉由施加（譬如配送施加 Kdit）進行

AF  
BT

## 五、發明說明（185）

及主導點，譬如根據使用記錄再生器與之相互關係或密約第 2 步生成主導點之構成。上道說明之認證處理（參考圖 2-2），係在副設置之內部記錄選擇先用以密約認證處理後作為構成，但將比如圖 5-5 所示在認證處理時根據主導點可修改為生成之構成。

譬如記錄再生器之副設置，係將認證處理開始前之初期化處理，在步驟 S 5-4-1 中，來源審核記錄與主導點之內部記錄後之主導點及密約 ID 用以生成認證點 Kake 使用於相互通訊處理，此係譬如，藉由 Kake = DES (MKake) 與密約 ID ) 進行認證處理。其次，步驟 S 5-4-2 中，將生成之後之認證點密約於記錄再生器。

另外，譬如在記錄再生器等之主導點，依步驟 S 5-4-3 中，將密約之後之記錄再生器，即由副設置，通過選取密約出副設置 ID。其次，步驟 S 5-4-4 中，根據選取後之副設置 ID 及所有之認證點生成用主導點以生成認證點密約使用於相互認證處理。該生成處理，係著如形容詞密約點 Kake = DES (MKake)、副設置 ID )。在步驟 S 5-4-5 中，使用密約認證點用以執行認證處理。

在該例中，如圖 5-5 下段所示，副設置、及主導點之雙方具有主導點，即認證點生成用主導點 MKake，在相互通訊處理必要的認證點分別逐行所有之主導點根據密約 ID 加以生成。

該系統，係萬一使認證點生成相應於第三步時，該認證點，係著其在相互通訊有效，所以在與其他兩個密約中

AF  
BT

## 五、發明說明（185）

帶密約化之步驟，步驟 S 5-3-3，係著如將密約化存儲信息寄納於記錄之記錄再生器。

另外，用以管理記錄再生器之系統管理名稱，係由用以密約化存儲信息之記錄再生器利用者或依據密約資料之密約，步驟 S 5-3-4 中，由記錄再生器，譜出記錄再生器 ID。其次，步驟 S 5-3-5 中，根據譜出後之記錄再生器 ID 及所有之主導點用以生成適用於密約化存儲信息之密約。該生成處理，係著存儲信息譯點 Kcon 時，則實質形成為存儲信息譯點 Kcon = DES (MKcon)、記錄再生器 ID )。在步驟 S 5-3-6 中，使用該密約用以譜存密約信息。

在該例中，如圖 5-4 下段所示，記錄再生器利用者、及系統管理名稱之力具有主導點（譬如存儲信息譯點生成用主導點 MKcon），在存儲信息之暗化、譯碼所必要的配送施加分別逐行所有之主導點根據各 ID（記錄再生器 ID ) 加以生成。

該系統，係萬一使存儲信息譯點生成相應於第三步時，係著該存儲信息之密約形成放在第三步，但為了可用以防止該密約化於記錄再生器 ID 之不同其他記錄再生器後之存儲信息的譯碼，可真有使 1 倍之存儲信息譯點之密約所影響到系統全體做為最小限度的效果。又，如一般管理所指，用者若要選擇兩者中，也真無必要以保持各存儲信息譯點之財別名單的效果。

圖 5-5 具有，即假設，譬如記憶卡等之記憶裝置，

AF  
BT

## 五、發明說明（187）

，使認證形不成不成立，由於始點之密約具有將產生之影響做為最小限度之效果。

如此，本發明之資料或理依據中，存儲信息提供者及記錄再生器，或記錄再生器及記錄密約僅僅之 2 個實體間中在有明顯地資料和密約之字樣將必要之聯繫等的實質由主導點及各 ID 依各密約需進行生成之構成。因此，使認證資訊由各實體即使於認證時，藉由借由密約化使存儲密約更密鎖定，又如前面古密約實體也形成不至密約名單之普遍。

## (1-3) 密約處理中之密約強度的控制

上述之實例中，在記錄再生器 300 及記錄密約 400 間之密約處理，係為了將說明容易理解，主要地，使用前兩項之密約之單 DES 構成對於使用密約處理之例做了說明。可是，本發明之資料處理依據中接適用於密約處理方式之上述之單 DES 方式不概任何限定，可應用以採用根據必要之安全狀態的增強化方式。

譬如象前面已說明之圖 8-1 至 10 之構成或採用三倍 DES 方式也可。譬如圖 3 所示在記錄再生器 300 及記錄處理器 400 之密約處理 401 中，密約可執行三倍 DES 方式之構成。在圖 8-1 至 10 之構成由已說明之三倍 DES 方式可構成用以執行對應於密約處理之處理。

可是，存儲信息提供者，依其存儲信息用以優先識別準度並將存儲信息譯點 Kcon 藉由單 DES 方式也有做為

AT  
BT

## 五、發明說明(180)

64位元地址構成的情形，又，用以優先安全作並將存儲器存儲地址 Kcon 由三倍 DES 方式也有做為 128 位元地址構成的情形，或做為 16 位元。因此，將記錄再生器 3 0 0 2 處理部 3 0 2，及記錄再生器 3 0 0 中之倍號處理部 4 0 1 之構成做為僅可對應於三倍 DES 方式，單 DES 5 方式其中之一方的方式之構成並較佳。因此，記錄再生器 3 0 0 之倍號處理部 3 0 2，及記錄再生器 4 0 0 之倍號處理部 4 0 1，係做為皆可對應的單 DES，三倍 DES 之構成為較佳。

可是，將記錄再生器 3 0 0 之倍號處理部 3 0 2，及記錄再生器 4 0 0 之倍號處理部 4 0 1 的階級處理構成為了僅能可對單 DES 方式，三倍 DES 方式之雙方的構成，併必須分別所以構成另外之路徑，邏輯。若在記錄再生器 4 0 0 中再有以執行對應於三倍 DES 之處理，係在於至圖 29 所示之指令地址必要形成將三倍 DES 之指令設定進步前的容納。此係帶來形狀構成於記錄後置 4 0 0 之問題的複雜化。

於是，本發明之資料或記憶體，係須申請將記錄後置 4 0 0 處之單倍處理部 4 0 1 再與之相連做為單 DES 構成，且可執行對應於三倍 DES 様化處理之處理，藉由三倍 DES 方式轉換化資料(資料、存儲信息)數路可容於記錄後置之外部記錄後置 4 0 2 的構成。

參照圖 3 2 所示資料格式形狀之例中，由記錄再生器 3 0 0 對記錄後置 4 0 0 用以執行存儲信息資料之下載

AT  
BT

## 五、發明說明(190)

或單 DES 方式以說明構成之流程圖，圖 5 6，係做為一個由記錄再生器 3 0 0 之存儲信息資料在記錄後置 4 0 0 進行下載操作用於執行保存地點 Kstr 之後之存儲信息地點 Kcon 的階級化處理時，顯示使存儲信息地點 Kcon 由三倍 DES 方式之階級化的情形，尚有，以此，存儲信息地點 Kcon 為代碼，顯示其虛擬性，但其虛擬性，存儲信息等，對於其他之資料也可同樣處理。

在三倍 DES 方式中，係如前圖圖 8 ～ 1 0 中已說明，以單 DES 係 64 位元地點，藉由三倍 DES 方式時，係做為 128 位元，或 1 92 位元之階級化構成，用 2 倍，或 3 倍之階級化處理。將此等 3 倍之存儲信息地點分別做為 Kcon 1 、 Kcon 2 、 (Kcon 3 )。 Kcon 3 也有未使用時，所用形狀顯示。

對於圖 5 6 之處理加以說明，步驟 S 3 0 1 係在記錄再生器 3 0 0 ，及記錄後置 4 0 0 之間相互對應步驟。該相互對應處理步驟，係須由前面已說明圖 2 0 之處理步驟執行。尚有，該認證處理時，使對話時間地點 Kstr 產生誤。

終了步驟 S 3 0 1 之認證處理，而在步驟 S 3 0 2 中，使各對應，核對地點 A 、核對地點 B 、存儲信息核對值，總核對値，各 I C V 之核對處理被執行。

終了之核對條件(I C V)判斷處理，則判定其是否，則跳到步驟 S 3 0 3，在記錄再生器 3 0 0 中，記錄再生器地點處理部 3 0 2 之控制部 3 0 6，係使用

AT  
BT

## 五、發明說明(189)

而，圖 3 9 係顯示前面已說明在格式形狀 0 之下系統處理的步驟 S 1 0 1 用以執行確認處理，於此用以生成對括時間地點 Kstr 、並面、步驟 S 1 1 7 中，在記錄再生器 3 0 0 之倍號處理部 3 0 2 裏由對話時間地點 Kstr 之存儲信息地點 Kcon 之階級化處理被執行，並使階級化處理始浩過訊號備考表送到記錄裝置 4 0 0 。步驟 S 1 1 8 中，接取新階級化論述後之記錄裝置 4 0 0 之階級處理部 4 0 3 藉由對話時間地點 Kstr 用以執行存儲信息地點 Kstr 之階級處理，並面，藉由與階級化 Kstr 用以執行存儲信息地點 Kcon 之階級化，並將此發送到記錄再生器 3 0 0 之階級處理部 3 0 2 之家，使記錄再生器 3 0 0 用以形成(步驟 S 1 2 1 )資料格式轉換化後之資料發送到記錄裝置 4 0 0 ，並使記錄裝置 4 0 0 將接收後之資料進行密寫於外部記憶體 4 0 2 。

上述處理中在步驟 S 1 1 7 、 S 1 1 8 間以簡易執行記錄裝置 4 0 0 之階級處理部 4 0 1 之階級處理部 4 0 0 以選擇可執行單 DES 、或三倍 DES 其中之一方式，則單 DES 信息提供者可以提供用根據三倍 DES 之存儲信息地點 Kcon 的存儲信息資料時，又用以提供用根據單 DES 之存儲信息地點 Kcon 的存儲信息資料時，對各種情形形態形成可對應。

圖 5 6 係顯示本發明之資料處理過程中使用記錄再生器 3 0 0 之倍號處理部 3 0 2 ，及記錄裝置 4 0 0 之階級處理部 4 0 1 之雙方用以執行根據三倍 DES 方式的增強

AT  
BT

## 五、發明說明(195)

記錄再生器地點處理部 3 0 2 之倍號／階級化部 3 0 8 ，並使用前面取出或生成後之記憶地點 Kdis ，通過接收後之地點 5 0 0 ，或，透過部 3 0 5 由通訊裝置 5 0 0 進行被容納於接收後之資料集管部的存儲信息地點 Kcon 之階級化處理。該情形之存儲信息地點 Kcon 係由三倍 DES 方式之階級，存儲信息地點 Kcon 1 、 Kcon 2 、 (Kcon 3 )。

其次，步驟 S 3 0 4 中，記錄再生器地點處理部 3 0 2 之控制部 3 0 6 ，係在記錄再生器地點處理部 3 0 2 之倍號／階級化部 3 0 8 中，在步驟 S 3 0 3 從河岸區隔後之存儲信息地點 Kcon 1 、 Kcon 2 、 (Kcon 3 )之中的存儲信息地點 Kcon 1 在相互認證時以進行共有啟動的對話時間地點 Kstr 進行階級化。

記錄再生器 3 0 0 之控制部 3 0 1 ，係以對話時間地點 Kstr 何時被階級化之存儲信息地點 Kcon 1 之資料由記錄再生器 3 0 0 之記錄再生器地點處理部 3 0 2 提出，將此等之資料透過記錄再生器 3 0 0 之記錄裝置控制器 3 0 3 送達至記錄裝置 4 0 0 。

其次，步驟 S 3 0 5 中，由記錄再生器 3 0 0 用以接收被發送回來之存儲信息地點 Kcon 1 之後之記錄裝置 4 0 0 ，係接收收後之存儲信息地點 Kcon 1 在記錄裝置處理部 4 0 1 之倍號／階級化部 4 0 6 ，相互通訊時以共有啟動的對話時間地點 Kstr 進行階級化，而面，在步驟 S 3 0 6 中，保存於記錄裝置地點處理部 4 0 1 之中記錄裝置 4 0 5 的記錄裝置有之存儲信息地點 Kstr 使再階級化。

五、發明說明（<sup>182</sup>）

流程圖表示 4 0 4 於發送記錄再生器 3 0 0 。

其次，步驟 S 3 0 7 中，記錄再生器號碼處理部

3 0 2 之控制部 3 0 0 G，係在記錄再生器號碼處理部

3 0 2 之串號／譯碼化部 3 0 8 中，以步驟 S 3 0 3 僅將

譯碼化後之存儲信息編址 Kcon 1 、 Kcon 2 、 ( Kcon 3 )

中之各項信息編址 Kcon 2 在相互認證時以進行共有放等

的對話並據此 Kcon 2 進行串號化。

記錄再生器 3 0 0 之控制部 3 0 1 ，係以對話時間統計 Kcon 2 將被串號化後之存儲信息編址 Kcon 3 之資料由記錄再生器 3 0 0 之記錄再生器號碼處理部 3 0 2 處出，並將此等之資料送進記錄再生器 3 0 0 之記錄再生器號碼處理部 3 0 3 並送至記錄號碼 4 0 0 。

其次，步驟 S 3 0 8 中，由記錄再生器 3 0 0 用以接收並將其而來之存儲信息編址 Kcon 2 後之記錄號碼 4 0 0 。

係將此收後之存儲信息編址 Kcon 2 在記錄號碼處理部 4 0 1 之串號／譯碼化部 4 0 6 、相互認證時以共有放等的對話時間統計 Kcon 2 進行譯碼化。繼而，在步驟

S 3 0 9 中，保存於記錄號碼處理部 4 0 1 之內部記憶體 4 0 5 的記錄號碼固有之存儲信息編址 Kstr 之存儲號碼，送進記錄號碼 4 0 4 並發送給記錄再生器 3 0 0 。

其次，步驟 S 3 1 0 中，記錄再生器號碼處理部

3 0 2 之控制部 3 0 0 G，係在記錄再生器號碼處理部

3 0 2 之串號／譯碼化部 3 0 8 中，以步驟 S 3 0 3 將

譯碼化後之存儲信息編址 Kcon 1 、 Kcon 2 、 ( Kcon 3 )

五、發明說明（<sup>194</sup>）

編址形成可進行容錯，如有，便存個位址編址 Kcon 係

Kcon 1 、 Kcon 2 之二級編址時，則步驟 S 3 1 0 ~ 3 1 2

之處理被省略。

如此，記錄號碼 4 0 0 、係多欄選擇之處理，即步驟 S 3 0 5 、 S 3 0 6 之處理步驟由複數次，係用以變更其對象進行處理執行，並三倍 D E S 方式用之將其形成可容於記憶體，存儲信息編址 Kcon 係存 D E S 之處理時，則用以執行步驟 S 3 0 5 ~ S 3 0 6 、並用以執行步驟 S 3 1 3 之格式化處理並容納於記憶體即可。如此之形成，係將以執行步驟 S 3 0 5 ~ S 3 0 6 之處理之權令納於前面已說明之圖 2 之附圖，將此處理藉由存儲信息編址之串號，即串由三組 D E S 方式，或單 D E S 方式，進行適當 1 次 ~ 3 次執行之構成即可。因此，在記錄號碼 4 0 0 之處理過程中不會三倍 D E S 之處理方式，形成可三倍 D E S 方式，單 D E S 方式，雙方之處理，與有，對於串號化方式，係依據於存儲信息資料之集管部內之處理方針，並將此加為參考而進行判斷。

( 1.4 ) 狀存儲信息資料之處理方針中之啓動優先順位之啟動順序處理

出前並已說明之圖 4 ~ 圖 6 的存儲信息資料構成能被理解，並請再者於本發明之資料處理裝置中被利用存儲信息資料的集管部之處理方針，並能合存儲信息狀態，即啓動優先順位資訊。本發明之資料處理裝置中之記錄再生器

五、發明說明（<sup>195</sup>）

之中的存儲信息編址 Kcon 3 在相互認證時以進行共有放等的對話時間統計 Kcon 2 進行理號化。

記錄再生器 3 0 0 之控制部 3 0 1 ，係以對話時間統計 Kcon 2 將被串號化後之存儲信息編址 Kcon 3 之資料由記錄再生器 3 0 0 之記錄再生器號碼處理部 3 0 2 處出，並將此等之資料送進記錄再生器 3 0 0 之記錄號碼處理部 3 0 3 並送至記錄號碼 4 0 0 。

其次，步驟 S 3 1 1 中，由記錄再生器 3 0 0 用以接收並送進來之存儲信息編址 Kcon 3 後之記錄號碼 4 0 0 、係將此收後之存儲信息編址 Kcon 3 在記錄號碼處理部 4 0 1 之串號／譯碼化部 4 0 6 、相互認證時以共有放等的對話時間統計 Kcon 2 進行譯碼化。繼而，在步驟 S 3 1 2 中，保存於記錄號碼處理部 4 0 1 之內部記憶體 4 0 5 的記錄號碼固有之存儲信息編址 Kstr 之存儲號碼，送進記錄號碼 4 0 4 並發送給記錄再生器 3 0 0 。

其次，步驟 S 3 1 3 中，記錄再生器 3 0 0 之各欄資料形式，並變更到記錄號碼 4 0 0 。

最後在步驟 S 3 1 4 中，記錄號碼 4 0 0 、係將其了格式形成之後之存儲資料寄送於外部記錄號碼 4 0 2 、該格式資料，係在保存編寫 Kstr 會有存儲號化後之存儲信息編址 Kcon 1 、 Kcon 2 、 ( Kcon 3 ) 。

藉由用以執行如此之處理，將寄納於記錄號碼 4 0 0 之存儲信息編址 Kcon 2 由三倍 D E S 方式之燒錄方式做為

五、發明說明（<sup>195</sup>）

3 0 0 、係使各記錄於記錄號碼 4 0 0 、或 D V D 、 C D 、硬碟，而進而啟動卡選項之各種記錄媒體後之可存取的存儲信息資料進行就讀等，將此等存儲信息之帶位依據優先優先級資訊加以決定。

記錄再生器 3 0 0 ，係各記錄從 D V D 標度， C D 標度，硬碟，確認各記錄資料中之優先順位資訊，用以優先並執行最高優先順位的存儲信息資料之中之序，以下對於該「根據在存儲信息資料之處理方針中的啓動優先順位之程序」能形容，如以說明。

上述之本發明的資料處理裝置實施例之說明中，係使記錄再生器 3 0 0 由 1 個之記錄號碼 4 0 0 存儲信息資料以進行再生、執行時之處理中心做了批判，可是，一般而言記錄再生器 3 0 0 、係如圖 2 所示除了記錄號碼 4 0 0 之外，通過讀取部 3 0 4 被連接 D V D 、 C D 、硬碟，進而通過 P I O 1 1 1 、 S I O 1 1 2 被連接記憶卡、記憶卡匣等，在各種記錄媒體具有可存取之構成，倘有，在圖 2，係為了避兔光圈之複雜化僅記載 1 個讀取部 3 0 4 ，但記錄再生器 3 0 0 、係將不同記憶媒體，譬如 D V D 、 C D 、收錄，瞭解以並列可嵌入。

記錄再生器 3 0 0 ，係可存取於復數之記憶媒體，在分別之記憶媒體間分別存儲資料並容納，譬如優

C D 等外部之各欄容易使用者進行供給存儲信息資料，係以前述之圖 4 的資料構成被容納於媒體，通過此等之媒體



A7  
B7**五、發明說明（200）**

信息之下載，並隨著再生處理，將臉部化資料之處理作為中心發明說明。

圖 3 之記錄再生器 3000 中之控制部 301，係由用以提供存儲信息資料之 DVD 等的讀寫頭 500，資訊美壓 600，記錄裝置隨著存儲信息資料之下載處理，或再生處理而以待封裝並處理，簡略化，詳述化處理全盤。

做為此等之處理結果並取得之可視存儲信息，係實如有聲音資料，圖像資料等。詳述資料係由控制部 301 放置於圖 2 所示主 CPU 之控制下，將圖像資料，圖音資料等被輸出到 A/V 輸出部。可是，使存儲信息譬如如有聲音資料時，M P 3 被形成，則藉由圖 2 所示 A/V 輸出部之 M P 3 被應用使圖音資料之詳述過程被形成並被輸出。又，使存儲信息資料關係圖音資料，並係由 M P E G 2 圖像圖音資料時，則藉由 A/V 处理部之 M F E G 2 認識部使存儲信息形成並被輸出。如此，被合於存儲信息資料之資料，係也有被轉換（符號化）或壓縮，又或是未被實施壓縮或處理之資料，所以實際根據存儲信息之亮度加以輸出。

可是，整體處理，伸長處理程式，有各種類的種類，由存儲信息提供者被提供圖音資料也無對應之伸長或重執行程式時，會產生將此不能進行再生之事態。

於是，本發明之實質或處理程度，係用表示在資料存儲信息中，一起用以容納圖音資料及其圖譜（伸長）處理程式之構成，或將圖音資料及選擇（伸長）處理程式之這些資訊從存儲信息資料之無聲資訊進行容納之構成。

本願狀及追加圖面審查請求書(CN1044萬卷(210+207公量)) - 203-

A7  
B7**五、發明說明（201）**

由圖 2 所示之東列處理全體圖，將有關本發明之要素及圖案要素以簡單圖面顯示於圖 60，記錄再生器

300，係由如 D Y D 、 C D 等之機械 500，或通訊裝置 600，或由用以容納存儲信息之後之記憶卡等之記錄裝置 400 接受機器之存儲信息之供給。此等之存儲信息，係有聲音資料，靜態影像，動態影像資料，從式資料等，又有實施唯聲化使用者，或未實施處理者，又，有被形成壓縮使用者，或未被形成者等，並管理之資料。

使存儲信息提供者被順序化時，係藉由如上所述之項目中已說明之方法被順序化部 301 之控制，及被處理部 302 之機器之處理部被順序處理並執行。被稱為此之資料係在主 CPU 106 之加速度下被順序到 A/V 處理部 109，並被容納於 A/V 處理部 109 之記憶體 3090，而在存儲信息解部 3001 中從存儲信息構成之解剖被執行，譬如在存儲信息中若被圖音資料伸長程式被選擇，則在程式記憶部 3093 用於某個程式，若被含有聲音資料，圖像資料等之資料則將此等資料於資料記憶部 3092，伸長處理部 3094，並嘗試使用被記憶於程式記憶部之後之 M P 3 等伸長處理程式用以執行被記憶於資料記憶部 3092 之後被更新的伸長處理，並被輸出到聲音器 3001，常為 3000 2。

其次，使 A/V 處理部 109 遵循控制部 301 之許可授受之資料之構成及處理參照之附加以說明，尚有，於此，做為存儲信息之例示顯示聲音資料，又做為壓縮程式之例

本願狀及追加圖面審查請求書(CN1044萬卷(210+207公量)) - 204-

A7  
B7**五、發明說明（202）**

將被用 M P 3 之壓縮程式或為代表前以說明，但本構成，係不僅聲音資料，也可適用於圖像資料。又，對於壓縮伸長處理度不不僅 M P 3，也可用以擴充 M P E G 2 、 4 等各類程式。

圖 6 1 係顯示存儲信息構成例，圖 6 1 係由 M P 3 伸長後收容之後之音頻資料 6 1 0 2 、 M P 3 認識（伸長）或程式 6 1 0 1 合併為 1 個之存儲信息構成之例。此等之存儲信息，係既為 1 位存儲資料於音頻 500，或記錄装置 400，或由通訊裝置 600 被配訊。記錄再生器 3000 、或將此等之存儲信息如前面已說明，若有被轉換化者，則藉由增設記憶部 3003 用以執行詳述處理後，並轉送到 A/V 處理部 109 。

在 A/V 處理部之存儲信息解部 30091，係用以解折後收容之存儲信息，由聲音資料伸長程式（ M P 3 認識器）等，及壓縮聲音資料所構成之存儲信息，用以取出聲音資料伸長程式（ M P 3 認識器）部並在程式記憶部 3093 用以記憶程式，將壓縮聲音資料記憶於資料記憶部 3092 时，尚有，存儲信息解部 30091，係依據存儲信息之外部資訊名稱等來存儲資料，資料長，資料傳達等用以執行存儲信息處理也可。其，伸長伸長或伸長部 30094，係依據依記憶於程式記憶部 3093 後之聲音資料伸長程式（ M P 3 認識器）用以執行被記憶於資料記憶部 3092 後之 M P 3 構

A7  
B7**五、發明說明（203）**

壓縮音頻資料之存儲信息處理，而 A/V 處理部 109 係伸長之後之聲音資料被輸出到聲音器 3001 。

圖 6 2 係顯示存儲部 6 1 顯示之存儲信息構成資料之再生處理一例之流程圖，步驟 S 6 7 1，係被容納於 A/V 處理部 109 之記憶體 3090 後之資料名稱，譬如若聲音資料之存儲信息則附以其名等之資訊與存儲信息另外接收之後資訊，或由存儲信息內之資料取出，並顯示於螢幕 3002。步驟 S 6 7 2，係將利用者之選擇由前面，統整等各種輸入裝置通過輸入接口進行接受，在 C P U 106 之控制下根據利用者輸入資料將再生處理指令輸出到 A/V 處理部 109。A/V 處理部 109，係在步驟 S 6 7 3 中藉由利用者選擇用以執行資訊之抽出，伸長處理。

其次圖 6 3 係顯示在 1 個之存儲信息被合組相容資料，或伸長處理程式之其中一方，而導致各存儲信息之集管資訊顯示存儲信息之內容含存儲信息資訊之構成。

如圖 6 3 所示，便存儲信息有程式 6 2 0 2 时，則收為無聲資料 6 2 0 1 有程式，及使程式壓縮器 6 2 0 2 伸長程式被含有存儲信息資訊資料。另外，將聲音資料 6 2 0 4 除為存儲信息合有的時，則在高音 6 2 0 3 之存儲信息資訊係由 M P 3 壓縮資料被含有資訊，該無聲資訊，譬如當前述之圖 6 4 所示由合於存儲信息資料構成之處理方針（參考圖 5 ）中的資料用以選擇僅在再生必要的資訊轉送至 A/V 處理部 109 並在存儲信息進行附加構成。

AF  
BT

## 五、發明說明（204）

具體而言，依在圖 5 所示「處理方針」中之各項資訊在唯讀部 30 0 2 中成為必要之或複雜方針資料，及在 A V 處理部 1 0 9 中在再生處理時成為必要之資料用以附加錄別值，使此項資訊僅在 A V 或複雜部 1 0 9 中惟若顯示必要者進行抽出可能為異常資訊。

圖 5 並示用以檢視各存儲信息後之 A V 或複雜部。

1 0 9 的存儲信息分析部 3 0 9 1，係依據重要資訊，有程式辨別將包式存儲信息記憶於資料記錄部 3 0 9 2。之後，壓縮部 3 0 9 3 將由資料記錄部用以取出資料，並依據記憶於程式記錄部 3 0 9 3 後之 S 5 3 程式用以執行伸長處理並加以抽出，而，在程式記錄部 3 0 9 3 便已經回一程式被召喚時，即程式式的處理策略也可。

圖 6 4 例顯示於有圖 6 3 所示存儲信息構成資料之再生處理的一例流程圖，步驟 S 6 7 5，係被召喚於 A V 或複雜部 1 0 9 之記憶體 3 0 9 0 後之資料分析，譬如若有音樂資料之存儲信息則將曲名等之資料與存儲信息另外接收後之資訊，或由存儲信息內之某處取出，並顯示於畫幕 3 0 0 2。步驟 S 6 7 6，係利用用以選擇由圖庫、樂曲等各項輸入裝置透過輸入埠口 1 0 0 進行接收。

其次，在步驟 S 6 7 7，係用以檢視對於利用者選擇之資料再生用程式（譬如 M P 3），該程式檢測到，係將記憶再生器 3 0 0 之存儲範圍作為最大檢索範圍而較佳，譬如圖 6 0 所示也將各選項 5 0 0，述說與圖

本說明文及適用於中國國家標準 GB/T15236-2009《公報》 - 207 -

AF  
BT

## 五、發明說明（205）

5 0 0，記錄装置 4 0 0 等也做為檢索範圍。

據此交於 A V 或複雜部 1 0 9 之存儲信息僅有資料部，程式存儲信息係也有被召喚於記錄再生器 3 0 0 內其他之記錄器體時，通過 D V D 、 C D 等之媒體而存儲信息提供者也有被提供。因此，將被召喚之象徵為檢索範圍用以記錄再生器 3 0 0 之存取容納範圍，從而後結果地發送再生程式，則在 C P U 1 0 6 之控制下根據利用者輸入資料將再生指令抽出於 A V 或複雜部 1 0 9 、 A C 處理部 1 0 9，並藉由步驟 S 6 7 9 中之利用者選擇用以執行資料之抽出，伸長處理。又，與前述的實例，其程式之检索在步驟 S 6 7 5 之終點行，步驟 S 6 7 5 中，使程 式區域能用以顯示並檢視後之資料也可。

據圖 6 5 例顯示在於圖 6 之存儲信息檢合有圖號齊音資料 6 3 0 3，並於或複雜部 6 3 0 2，進而做為存儲信息之象徵資訊 6 3 0 1 被含有存儲信息之再生優先級判斷的檢測例。此係，在前圖圖 6 1 之存儲信息檢合程式檢索資料用以附加再生優先級之資訊之例。此係，與前述之「（14）存儲信息資料中根據處理方式中之優先級而較低的程式啟動處理」同樣，在步驟 A V 或複雜部 1 0 9 之後之存儲信息檢合被設定後之再生優先順位用以決定再生順序。

圖 6 6 例顯示持有圖 6 5 例示存儲信息構成資料之再生處理的一例流程圖，步驟 S 6 8 1，係被召喚於 A V 或複雜部 1 0 9 之記憶體 3 0 9 0 後之資料，即將再生對象資訊之優先級被定後之再生優先順位用以決定再生順序。

本說明文及適用於中國國家標準 GB/T15236-2009《公報》 - 208 -

AF  
BT

## 五、發明說明（206）

該之資料資訊設定於檢索名單，檢索名單係使用 A V 或複雜部 1 0 9 之之記憶體的一部分領域進行設定。其次，步驟 S 6 8 2 中，由 A V 或複雜部 1 0 9 之存儲信息解析部 3 0 9 1 中的檢索名單用以選擇高優先順位之資料，並在步驟 S 6 8 3 中，用以執行並選擇之後之資料之再生處理。

其次圖 6 7 例顯示在 1 例之存儲信息由皇管資訊及程式資料 6 4 0 2，或集管資訊 6 4 0 3，及初期資料 6 4 0 4 中之其中之一組合所構成的，而，在資料存儲信息之氣氛 6 4 0 3，該附加有再生優先順位資訊之構成例。

圖 6 8 例顯示持有圖 6 7 例示存儲信息檢合之再生處理的一例流程圖，步驟 S 6 9 1，係被召喚於 A V 或複雜部 1 0 9 之記憶體 3 0 9 0 後之資料，即將再生對象資訊之資料資訊設定於檢索名單，檢索名單係使用 A V 或複雜部 1 0 9 之記憶體的一部分領域進行設定。其次，步驟 S 6 9 2 中，主 A V 或複雜部 1 0 9 之存儲信息分析部 3 0 9 1 中的檢索名單用以選擇高優先順位之資料。

其次，在步驟 S 6 9 3，係用以檢視對象於被選擇後之資料之資料再生用程式（譬如 M P 3），該程式檢測到，並因前至步驟 6 4 之流程圖中之處理同様，若記錄再生器 3 0 0 之存儲範圍較廣為最大檢索範圍為較佳，譬如也持圖 6 0 所示各選擇 5 0 0，訊訊装置 6 0 0，記錄裝置 4 0 0 等為檢索範圍。

當為檢索結果找到再生程式（在步驟 S 6 9 4  
Y e s），則在步驟 S 6 9 5 中，將被選擇後之資料使用

AF  
BT

## 五、發明說明（207）

檢索結果被取得之程式，用以執行伸長再生處理。

另外，故為被檢索結果程式被抽離時（在步驟 S 6 9 4 Y e s），則進到步驟 S 6 9 6，在步驟 S 6 9 1 被告於設定後之檢索名單中之其他資料，使用同一程式之再生處理用以檢視必要的資料。此係，由於明白顯示對新的該資料即使用以再生程式檢索但未被換出，進而，在步驟 S 6 9 7 中用以判定後檢索名單是否空的，非空的情形，則返回到步驟 S 6 9 2，並而用以抽出次次的優先順位之資料，所以執行程式檢索處理。

如此，若依據不構成，則被壓縮處理後之檢索信息，與其詳述（伸長）程式一起被稱呼，或僅存儲信息檢索統計之資料，或僅僅有其檢索處理程式時，則分別在存儲信息具有皇管資訊顯示存儲信息有如何之屬性資料，並用以執行如何之處理，所以僅存儲信息之後之處理部（譬如 A V 或複雜部），僅使用財惠於皇管資料之伸長處理用以執行伸長再生處理，或將伸長處理程式直接將該資料之無皇管資訊進行檢索，並因僅存儲結果被取得之程式用以執行伸長再生處理，所以難由利用者成為不需要資料之伸長程式的產生，檢索等處理用利用者負責被減輕，可形成有效的資料再生，進而，在檢索資料依據具有再生優先順位資訊之構成，則將再生順序形或可自動設定之構成，難由利用者可檢索再生順序設定之操作。

與有，上述之實例，係做為壓縮聲音資料存儲信息，及聲音壓縮資料之其處理程式將 M P 3 做為例子做了

A7  
B7**五、發明說明 (208)**

說明：若非那具有合逕資料存儲信息，壓縮圖像資料之伴員處理程式之存儲信息同樣也可應用本構成，可達成同樣效果。

**(16) 對存儲資料之生成及記錄裝置的密納，再生處理**

本發明之資料處理裝置，依密納之記錄再生器 3000 中並執行之存儲信息有逆載程式等情況等，可將右列逆載程式在中進行中斷，預定時間後，若重複再開時，並若其中觸及到點之遊戲狀態等存儲，即重新於記錄裝置，並將此在再開時進行譯出用以播放遊戲之構成。

首先之遊戲機器，個人電腦之記錄再生器中之存儲資料保存構成，並當如內藏於記錄再生器，或持有在可外附之記錄卡。收錄，遊戲主機，並錄音等之記錄體用以保存存儲資料之構成。依密納，對存儲資料未具有完全性確保構成，譬如在逆載應用程式以共同之規格形成並行實現之存儲處理之構成。

因此，譬如使用某 1 次之記錄再生器 A 發生被使用，或被遺忘之意思，先就，存儲資料之完整性無乎被考慮存儲狀況。

本發明之資料處理裝置，係用以提供可實現如此之存儲資料之完全性確保的構成。實若某遊戲程式之存儲資料，係備有記錄裝置或根據可使用之資訊進行準確化並密納之記錄裝置。或，根據記錄再生器有之資訊進行準確化並密納之記錄裝置。藉由此等之方法，將存儲資料之利用

A7  
B7**五、發明說明 (209)**

僅可限制在特定之機器，特定之程式，使存儲資料之完全性被確保。以下，對於本發明之資料處理裝置中之「對存儲資料之生成及記錄裝置之密納，再生處理」以說明。

圖 6 9 係顯示對於本發明之資料處理裝置中之存儲資料密納處理加以說明之方框圖。由 D V D 、 C D 等之媒體 5 0 0 0 ，或流訊裝置 6 0 0 0 使存儲信息被提供到記錄再生器 3 0 0 0 ，並提供存儲信息，係當由如前面說明之存儲信息固有神經之存儲信息總匙 K e y s 被轉化為記錄再生器 3 0 0 0 ，係在前述之 (7) 由記錄再生器對記錄裝置之下載處理」之欄依據說明（參照圖 2 2 ）之流程用以取得存儲信息總匙，並將密納化之存儲信息進行譯碼時，資訊於記錄裝置 4 0 0 0 。於此，係使記錄再生器 3 0 0 0 使存儲信息程式由硬盤，或流訊裝置加以譯碼並進行再生，執行，執行後，將被取得存儲資料外接，或寄給於內藏之記憶卡，硬盤等之各部記錄裝置 4 0 0 0 A 、 4 0 0 0 B 、 4 0 0 0 C 之其中之一，在再生處理，或將存儲信息在記錄裝置 4 0 0 0 A 上進行下載之後，由記錄裝置 4 0 0 0 A 用以再生，執行存儲信息，並當其存儲信息外接，或寄給於內藏之記憶卡，便傳送之名稱記錄裝置 4 0 0 0 A 、 4 0 0 0 B 、 4 0 0 0 C 之其中之一，並密納於處理記錄裝置 4 0 0 0 ，對於再生之處理加註說明。

記錄再生器 3 0 0 0 ，係當前項已說明具有用以生成記錄再生器基底總匙 1 D d e v ，在系統共同之名稱總匙的系統總匙 K e y s ，在這個之記錄再生器有之名稱總匙的記錄再

▲此版式是適用中國國家標準(CNS)A4紙面(210×297公釐) - 211 -

A7  
B7**五、發明說明 (210)**

生基底總匙 K e y s ，進而各種之類別與點的主總匙。對於主總匙，係在「(12) 標準主總匙之種類與總匙生成構造」中，如已詳細之說明，譬如，用以生成記錄裝置 K e y s ，或認證裝置 K a k e 等之總匙。於此，並無特別用以規定主總匙之種類須用以代表記錄再生器 3 0 0 0 具有之生產總匙之類似以 M X 加以顯示，在圖 6 9 之下段，係顯示存儲資料與總匙 K a k e 之例。平時資料與總匙 K a k e ，係將存儲資料於各種記錄裝置 4 0 0 0 A ∼ C 時之準確化處理，而且由各種記錄裝置 4 0 0 0 A ∼ C 被使用於再生時之譯碼處理的順序統一，並用圖 7 0 以下，用以說明存儲資料之容納之處理及再生處理。

圖 7 0 係使用存儲信息總匙，系統共同總匙之其中之一並將存儲資料容納於記錄裝置 4 0 0 0 A ∼ C 之中之一的處理資訊圖。實有，各總匙中之處理係執行記錄再生器 3 0 0 0 之處理。在各此用以容納存儲資料之記錄裝置內藏，若有外接記錄裝置 4 0 0 0 A ∼ C 之中之一部可，並無何被限制。

步驟 S 7 0 1 ，係將存儲信息總匙子，譬如若遊戲

I D 使記錄再生器 3 0 0 0 證出之處理。此係，前項已說明之圖 6 9 、 2 6 、 2 7 、 3 2 、 3 3 ∼ 3 5 所示被合於存儲信息資料中之識別資訊的資訊，將存儲資料之容納處理後合送過圖 2 9 所示輸入接口 1 1 0 ，使得產生之 C P U 1 0 6 第存儲信息識別子之採取指示的控制器 3 0 1 。

控制器 3 0 1 ，係當執行程式通過 D V D 、 C D ∼

A7  
B7**五、發明說明 (211)**

R O M 等，讓讀部 3 0 4 被執行的存儲信息時，則通過讓取部 3 0 4 取出整合於存儲信息資料中之無類的識別資訊，並使執行程式，被容納於記錄裝置 4 0 0 0 B 之存儲信息時，則通過記錄裝置控制器 3 0 3 3 取出識別資訊，俾當，使記錄再生器 3 0 0 0 使存儲信息程式在執行中，已在記錄再生器中之 R A M ，其他可存記錄裝置僅存儲信息識別子在宿端萬能時，則不執行新的獲取處理，而利用被合於識別完成資訊之識別資訊也可。

其次，步驟 S 7 0 2 ，係當由密納進行程式之使用限制以用於存儲信息之步驟。所謂程式使用限制，係當存儲之存儲資料僅在其程式所為據有可利用用以設定對有限制的限制資訊，僅當此為滿有可利用用以設定為「有程式使用限制」，並僅當在程式將未被拘來用於存儲資訊時被西「無程式使用限制」。此係，使用者做為可任意設定也，並當存儲資訊製作者進行設定，將該資訊容納於存儲信息程式中啟動也可，被設定後之限制資訊，係在圖 6 9 之記錄裝置 4 0 0 0 A ∼ C 係為資料管理推進被容納。

資料管理總匙之例顯示於圖 7 1 ，資料管理惟需係能為項目並能為合適資料號碼，存儲信息識別子，記錄再生器識別子，程式並使用限制之匯合於生成，存儲信息識別子，並形或用以容納存儲資料之對象之後之存儲信息式的識別資訊。記錄再生器識別子，係當有圖 6 9 所示 (1 D d e v ) ，程式使

▲此版式是適用中國國家標準(CNS)A4紙面(210×297公釐) - 212 -

## 五、發明說明 (212)

用限制：係如上述將存儲之存儲資料僅在其程式做為固有可使用時，則被認為「做」之設定，而未被限制對應程式做為可用時則形成「不做」之設定，程式使用限制，係用以利用存儲信息程式使使用者可在存儲資訊，並使存儲信息製作者進行設定，將該資訊寄存於存儲信息程式中故著也可。

退而步驟 7 0，繼續流程之說明，在步驟 S 7 0 2 中，對於程式使用限制被形成「做」之設定時，進到步驟 S 7 0 3、步驟 S 7 0 3，係由存儲信息資料譜出存儲信息也有之論點，譬如譜出前已說明之存儲信息驗匙 Ksav 並存儲信息圖有論點被為存儲資訊而被驗匙 Ksav，或根據存儲信息圖有論點被為存儲資訊而被驗匙 Ksav。

另外，步驟 S 7 0 2 中，對於程式使用限制被設定「不做」時，則退到步驟 S 7 0 7，在步驟 S 7 0 7，係被容納於記錄再生器 3 00 內之後之系統共同論點，譬如將系統署名識匙 Keys 由記錄再生器 3 00 之內部記憶體 3 0 7 進行譜出，將系統署名識匙 Keys 作為存儲資料而被驗匙 Ksav，或根據系統署名識匙能以生成存儲資料而被驗匙 Ksav，或，另外，存儲於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著，其與其之論點被別的論點驗匙被為存儲資料而被驗匙 Ksav 也可。

其次，步驟 S 7 0 4 中，以步驟 S 7 0 3，或步驟 S 7 0 7 選擇，或使用被生成後之存儲資料而被驗匙 Ksav 用以執行存儲資料之編號化處理，詳論號化處理，係使用

本說明文適用於中華民國標準(CNS)AA規範(210~217公尺) - 215-

## 五、發明說明 (214)

係存儲信息驗匙子使用不同程式時，又，將記錄再生器不同時進行再生形可利用。

圖 7 2 係顯示流程由圖 7 0 之存儲資料而被應用以再生被容納之後之存儲資料處理之流程圖。

步驟 S 7 1 1，係存儲信息識匙子，譬如將遊戲 ID 以及記錄再生器 3 0 0 譜出或退。此係，其前面已說明之圖 7 0 的存儲資料而被應用之步驟 S 7 0 1 同樣之處理，若該命令於存儲信息圖有論點被別的資訊的資料譜出處理。

其次，在步驟 S 7 1 2，係由圖 6 9 所示記錄裝置 4 0 0 A ~ C，並用圖 7 0 譜出或說明之資料管理檔案，並在步驟 S 7 1 1 中所以上述出之後之存儲信息識匙子，及進行判斷甚麼設定之後之程式使用限制資訊，使被設定於資料管理檔案之後之程式使用限制有「做」時，則進到步驟 S 7 1 4，有「不做」時，則進到步驟 S 7 1 7。

步驟 S 7 1 4，係由存儲信息資料而被譜出存儲信息圖有論點，譬如用以譜出前已說明之存儲信息驗匙 Ksav 並存儲信息圖有論點被為存儲資料而被驗匙 Ksav，或存儲存儲信息圖有論點被為存儲資訊而被驗匙 Ksav，該譜兩化論點生或處理，係成因於將論號化論點生成為論點並應用論號化論點，根據某存儲信息驗匙而被稱為被稱為存儲資訊而被譜兩化論點生成為論點並應用論號化論點生成為論點。

另外，步驟 S 7 1 2 中，從資料管理檔案之設定對於程式使用限制設定有「不做」時，則在步驟中 7 1 7 中，

本說明文適用於中華民國標準(CNS)AA規範(210~217公尺)

本說明文適用於中華民國標準(CNS)AA規範(210~217公尺) - 217-

## 五、發明說明 (213)

2 中之暗號化處理部 3 0 2 舊如用以應用並執行前述 D E S 算法。

步驟 S 7 0 4 中被暗號化處理後之存儲資料，係被容納於步驟 S 7 0 5 中之記錄裝置，將存儲資料後可容納之記錄裝置而被譜出圖 6 9 所示具有標數時，則使用前述記錄裝置 4 0 0 A ~ C 之中之一筆存儲資料官銷對象預先進行選擇，進而，在步驟 S 7 0 6 中使用的圖案 7 1 在於明之資料管理檔案之前而步驟 S 7 0 2 設定後之程式使用限制資訊之寫入，即用以執行程式使用限制「做」或「不做」的寫入。

以上，從存儲資料之折新處理進行終了。步驟 S 7 0 2 中之 Yes，即「進行程式使用限制」之選擇被形成，根據步驟 S 7 0 3 中之存儲信息圖有論點藉由產生之後之存儲資料而被驗匙 Ksav，該暗號化之存儲資料，係由未存儲存儲信息圖有論點資訊之存儲信息程式形成不可識識證匙，存儲資料所具備之存儲信息驗匙資訊而僅可利用存儲信息程式，但，於此，存儲資料而被驗匙 Ksav 係根據紀錄裝置圖有之資訊來生成，所以譬如被容納於記錄卡等之可識別的紀錄單張之後之存儲資料係在不同記錄單張中也與對應之存儲信息程式一起進行應用而形而可再生。

又，步驟 S 7 0 2 中之 No，即被形成「不做程式使用限制」之選擇，根據步驟 S 7 0 7 中之系統共同論點而由存儲資料而被驗匙 Ksav 被暗號化處理後之存儲資料

本說明文適用於中華民國標準(CNS)AA規範(210~217公尺) - 216-

## 五、發明說明 (215)

亦於於記錄再生器 3 0 0 內之系統共同論點，譬如將系統署名識匙 Keys 由記錄再生器 3 0 0 之內部記憶體 3 0 7 譜出，並非系統署名識匙 Keys 作為存儲資料而被驗匙 Ksav，或根據系統署名識匙 Keys 用以生成存儲資料而被驗匙 Ksav。又，另外，係存於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著，與其他存儲信息而被別的論點被以為存儲資料而被驗匙 Ksav 之使用也可。

其次，步驟 S 7 1 5 中，以步驟 S 7 1 4，或步驟 S 7 1 7 選擇，或使用被生成後之存儲資料而被驗匙 Ksav 用以執行存儲資料之暗號化處理，在步驟 S 7 1 5 中，將該命令之後之存儲資料在記錄再生器 3 0 0 中進行再生，執行。

在以上，按存儲資料之再生處理進行終了。如上述在資料管理檔案被形成有「進行程式使用限制」時，則根據存儲信息圖有論點被生成存儲資料而被驗匙，將並有「不進行程式使用限制」時，則根據系統共同論點而存儲資料而被驗匙並生成，被設定有「進行程式使用限制」時，則使用之存儲信息之存儲信息識匙子不相符合而形成不能取得存儲資料之譜兩化論點的譜兩化論點，形成可挑出存儲資料之安全性。

圖 7 3，圖 7 4 係使用存儲信息識匙子用以生成存儲資料之譜兩化論點，譜兩化論點之存儲資料而被應用於程圖 (圖 7 3)，存儲資料而被譜兩化論點 (圖 7 4)。

圖 7 3 中，步驟 S 7 2 1 ~ S 7 2 2，係與圖 7 0 之

本說明文適用於中華民國標準(CNS)AA規範(210~217公尺) - 217-

五、發明說明（<sup>218</sup>）

步驟 S 7 0 1 ~ S 7 0 2 同樣之處理，所以省略說明。

圖 7 3 之存儲資料容納處理流程，係步驟 S 7 2 2 中進行「進行程式使用限制」時，在步驟 S 7 2 3 中由存儲資訊寫入存儲資訊別子，即用以產生存儲信息 I D 並消存儲信息 I D 作為存儲資料識別號碼 Ksav，並根據存儲信息 I D 用以生成存儲資料識別號碼 Ksav。譬如記錄再生第 3 0 0 之場號處理步 3 0 7 係由存儲資訊別子在讓出存儲信息 I D 後，選用被容納於記錄再生器 3 0 0 之內部記錄後之主記錄 MKX，譬如藉由 D E S C M K X，在該信息 I D ) 可取得存儲資料識別號碼 Ksav。或，另外，保存於記錄再生器 3 0 0 之內部記錄步 3 0 7 之故案，與其他論點將列的結構論點做為存儲資料識別號碼 Ksav 使用也可。

別外，步驟 S 7 2 2 中，對於程式使用限制做為「不做」時，則步驟 S 7 2 7 中，被容納於記錄再生器 3 0 0 內之系統共用論點，譬如將存儲資訊別子 Ksav 由記錄再生器 3 0 0 之內部記錄步 3 0 7 跳出，並將系統共用名稱別子 Ksav 依為存儲資料識別號碼 Ksav。或根據存儲資訊別子用以生成存儲資料識別號碼 Ksav。或，另外，係於記錄再生器 3 0 0 之內部記錄步 3 0 7 之故案，與其他論點將列的結構論點做為存儲資料識別號碼 Ksav 使用也可。

步驟 S 7 2 4 以下之處理，係與前述之圖 7 0 的處理流程中之步驟 S 7 0 4 以下之處理同樣，所以省略說明。

進而，圖 7 4 係以圖 7 3 之存儲資料容納處理流程用

五、發明說明（<sup>218</sup>）

以設說要不進行記錄再生器之限制的步驟。記錄再生器限制，係用以限制可利用存儲資料之記錄再生器時，即用以生成存儲資料值在察後之記錄再生器做為可利用時設定為「做」。而在其他之記錄再生器做為可利用時進行設定為「不做」。步驟 S 7 4 2 中進行設定「進行記錄再生器限制」，則進到步驟 S 7 4 3，進行設定「不做」，則進到步驟 S 7 4 7。

再者，資料管理檔案之剖面顯示於圖 7 6。資料管理檔案係為項目合資料號碼，存儲資訊識別子，記錄再生器識別子，記錄再生器限制做為存儲去識別子，存儲資訊識別子，係成為用以容納存儲資料之對象之各存儲資料識別子之識別子。記錄再生器識別子，係用以容納在存儲資料後之記錄再生器識別子，譬如圖 8 所示之「IDkey」。記錄再生器限制，係用以限制可利用存儲資料之記錄再生器時，即用以生成存儲資料值在察後之記錄再生器做為可利用時進行設定「做」，而在其他之記錄再生器也將做為可利用時進行設定「不做」。記錄再生器資訊，係利用存儲資訊程式做利用者可任意設定也可，並使存儲資訊製作者進行設定，將該資訊容納於存儲信息裡式中就做也可。

圖 7 5 之存儲資料容納處理流程，係步驟 S 7 4 2 中，進行「進行記錄再生器限制」之設定時，在步驟 S 7 4 3 中由記錄再生器 3 0 0 用以生成記錄再生器認同有論點，譬如將記錄再生器名稱號碼 Kdev 由記錄再生器 3 0 0 之內部記錄步 3 0 7 跳出並將記錄再生器名稱號碼 Kdev 使用也可。

五、發明說明（<sup>217</sup>）

以再生、執行並客納於記錄再生器之存儲資料的處理流程，步驟 S 7 3 1 ~ S 7 3 3 係與前述圖 7 2 之對應處異同，惟僅步驟 S 7 3 4 不同。步驟 S 7 3 4 中，係存儲資訊資料用以讓出存儲資訊別子，即用以讓出存儲信息 I D 並將存儲信息 I D 作為存儲資料識別號碼 Ksav，或根據存儲信息 I D 用以生成存儲資料識別號碼 Ksav。該論點為化論先生成處理，係被適用於對應於前述化論先生成處理之處理算法，據此某存儲資訊別子藉由被稱化論先生成處理，並根據同一之存儲信息識別子藉由被生成之後之論點而得，或可證明該論點為化論先生成處理算法。

以下之處理，步驟 S 7 3 5 ~ S 7 3 6 ~ S 7 3 7，係與圖 7 2 之對應處理同樣所以省略說明。依據圖 7 3，圖 7 4 之存儲資料容納處理流程，則進行程式使用限制之設定時，用以使用存儲信息 I D 並係為用以生成存儲資料識別號碼 Ksav，據此化論先生成處理，所以與使用前而之存儲信息還有始於存儲資料識別子，再生處理同樣，使用前之存儲信息程式進行整合情形以外，係形成不能利用存儲資料之構成，成為可與存儲信息存儲資料完全一致。

圖 7 5 中，步驟 S 7 4 1，係與圖 7 0 之步驟 S 7 0 1 同樣的處理，所以省略說明。步驟 S 7 4 2，係

五、發明說明（<sup>218</sup>）

Kdev 為存儲資料識別號碼 Ksav，或根據記錄再生器名稱號碼 Kdev 用以生成存儲資料識別號碼 Ksav。或，另外，係存於記錄再生器 3 0 0 之內部記錄步 3 0 7 放置，與其他論點將列的論點做為存儲資料識別號碼 Ksav 使用也可。

另外，步驟 S 7 4 2 中，對於記錄再生器限制當為設定「不做」時，係在步驟 S 7 4 7 中，被容納於記錄再生器 3 0 0 內後之系統共用論點，譬如將存儲資訊別子 Ksav 由記錄再生器 3 0 0 之內部記錄步 3 0 7 進行選出，並將系統名稱號碼 Ksav 依為在存儲資料識別號碼 Ksav，或根據系統名稱號碼 Ksav 用以生成存儲資料識別號碼 Ksav。或，另外，保存於記錄再生器 3 0 0 之內部記錄步 3 0 7 放置，與其他論點將列的論點做為存儲資料識別號碼 Ksav 使用也可。

步驟 S 7 4 4 ~ S 7 4 5 之處理，係與前述之圖 7 0 的處理中之對應處理同樣，所以省略說明。

在步驟 S 7 4 6，係在資料管理檔案（參考圖 7 6）商存入存儲資訊識別子，記錄再生器識別子，而且在步驟 S 7 4 2 使利用者寫入設定後之記錄再生器啟動資訊「做／不做」。

進而，圖 7 7 係在圖 7 5 之存儲資料容納處理流程用以再生，執行並客納之後之存儲資料的處理流程圖；步驟 S 7 5 1 係與前述之圖 7 2 的對應處理同樣，用以讓出存儲信息識別子。其次，步驟 S 7 5 2 中，係用以讓出存

## 五、發明說明 (220)

在步驟 S 753，係由資料管理審核其（參考圖 76）。用以指出存儲信息識別子，記錄再生器識別子，設定完成之記錄再生器限制資訊「啟」不啟」之各資訊。使資料管理處置庫中之存儲信息識別子進行一致的項目中，使記錄再生器限制資訊被設定於「啟」時，則相關之項目之記錄再生器識別子在步驟 S 752因被讀取而之後記錄再生器識別子即因時刻進行了處理。

其次，在步驟 5754 使實業管理檢定之設定期「進行記錄再生器限制」時，則進到步驟 5755，有「不做」時，則進到步驟 5758。

步驟 S 7 5 5 中，係由記錄再生器 3 0 0 用以譯出紀錄再生器有論，譬如記錄再生器再生名稱號 Kdev 由記錄再生器 3 0 0 內之記錄記憶體 3 0 7 進行譯出並產生再生名稱號 Kdev 為存儲資料庫而稱號 Ksav，或根據記錄再生器再生名稱號 Kdev 以用以存儲資料庫而稱號 Ksav。譯出再生化號生成處理，係根據用對應於物理地址而稱號化號生成處理的處理算則。根據記錄再生器有論有論號被譯成化號之資料，併根據同一之記錄再生器有論號而稱號由前生後之時譯出論號而稱號可謂譯者並用譯產生化號而稱號生成論號。或，另外，係存於在紀錄再生器 3 0 0 之內部記憶體 3 0 7 內裝置，其與其餘號別而稱號號為存儲資料庫而稱號 Ksav... 依類推。

本试验风速选择中数据采样率 (CNS)A4 规范 (210~207 公里) - 223 -

五、發明說明 (222)  
傳存體資料將號繪寫  $K_{\text{av}}$  等。或，另外，保存於記錄再生器 3-0-0 之內部記憶體 3-0-7 內放著，與其他繪寫將別的印號繪寫放存個資料將號繪寫  $K_{\text{av}}$  用處也可。

以下之處理步驟 S765~S768，係與前述圖 2.5 之處理步驟相似，所以省略說明。

圖 7-9 係藉由圖 7-8 之處理用以再生，執行於容納於記憶裝置後之存儲資料的處理流程圖。步驟 S-771~

在步驟 S 775，係將記憶再生器置於復原之後之記錄再生器而離子  $\langle \text{Idev} \rangle$  並以生成存儲資料譯碼化離子  $\text{Kxx}$ ，將  $\text{Idev}$  留為存儲資料譯碼化離子  $\text{Kxx}$  進行適用，並以適用來尋找於記錄再生器 2'000 之內部記憶體之後之離子  $\text{MKx}$ ，藉由  $\text{DES}(\text{MKx}, \text{Idev})$  取得存儲資料譯碼化離子  $\text{Kxx}$  之後，依據  $\text{Idev}$  用於生成存儲資料譯碼化離子  $\text{Kxx}$ ，該運算離子生成或逕消，係將運算對應於單獨化離子生成運算之處理算法，根據某記錄再生器離子而被單獨化之後之資料，並根據圖二之記錄再生器離子而藉由步驟之後之譯碼化離子成為可譯讀者並適用譯碼化離子再生算法，另，另外，保存於記錄再生器 3'000 之內部記憶體 3'079 之放棄，與其他論述所別的離子離子而做為存儲資料譯碼化離子而應用。

以下之處理步驟 S776 ~ S778，係與前述圖

圖 7-8、圖 7-9 所示之存儲資料容納，若依據再生生成

五、參照圖(221)

另對多群 S 758 中，係依容納計紀錄再生得 300 之後之共通編址，譬如將系統名稱硬體 Ksys 由紀錄再生 300 之中內記憶體 307 運行譯出，甚麼系統名稱硬體 Ksys 係為存資料庫硬體 Ksav，或根據系統名稱硬體以生成存資料庫硬體 Ksav。又，另外，在於記錄再生 300 之中內記憶體 307 內，當其與編址所對應的硬體編址也存在資料庫硬體 Ksav 使用時，可以，以下之多群 S 758、S 757，係與前述之存資料庫再生此後，此後之財務管理模塊的運作。

圖 75、圖 77 所示之存儲資料，若依據再生處理流程，則被形成「進行記錄再生器限制」之選擇後的存儲資料，係藉由記錄再生器固有論點，為了被執行唯讀化，詳述化處理，持有一同一之記錄再生器固有唯讀化的記錄再生器，即僅看由同一之記錄再生器造成可利用進行詳述。

其次，圖 7-8、圖 7-9 係顯示使用記錄再生器識別子用以生成存儲資料哈希化，譯碼化檢點並進行容納，再生之處理。

圖 7-8 係使用記錄再生器識別子進行存儲資料之識別並審核於記錄裝置。步驟 S 7-6.1 ~ 7-6.3，備齊前面圖 7-5 同樣之處理。在步驟 S 7-6.4，係使用由記錄再生器提出後之記錄再生器識別子 (IDev) 能以能以存儲資料識別號論述 Kisv，將 IDev 做為存儲資料識別號給 Kisv 進行使用。並以適用被審核於記錄再生器第 3-0 之內部記憶體之後之主識別號 MX，藉由 D (M/K) = [IDev] + Kisv 進行推算。

名都娱乐有限公司之附属公司 (C286) 04 展场 (E201-E202 合共 2) - 224 -

五、時間相關 / 223

程規式，用被形成「進行記錄再生器限制」之選擇後的存儲資料，係當由記錄再生器選出誰此，為了被執行理賃化、運算化處理，將有同一之記錄再生器選出即為記錄再生器，則應由同一之記錄再生器所形成可利用選擇。

其次使用量 80 ~ 82，將上述之程式使用限制，及記錄再生器使用限制合併進行執行對於存儲資料，而生成

圖 8-0 例存儲資料容納處理。步驟 S 7-8-1 中，若存儲信息與子由存儲信息資料讀出，步驟 S 7-8-2 中，進行程式使用兩制判定。步驟 S 7-8-3 中進行記錄再生等項判定列。

「有程式使用限制」且「有記錄再生等限制」時，係在步驟 S 7-8-5 中，根據存儲信息有無被編（*x-Kcon*），及記錄再生等有無被編（*Ksav*）隻方產生或存儲資料塊地圖編號 *Ksav*。此係，若  $Ksav = (x-Kcon \text{ XOR } Ksav)$ ，或用以透過兼容符記錄再生等 300 之內部記錄後之主編此  $MKx$  為是基於  $Ksav = DES(MKx, Kcon \text{ XOR } Ksav)$  可取到；或，另外，保存的記錄再生等 300 之內部記錄 30-7 內啟動，與其總編址將別的單號編號然為存儲

「有程式使用限制」且「無記錄再生器限制」時，依在步驟 S786 中，將存儲信息區有論匙（ex.Kcon）做為存儲資料號址論匙 Ksav，或根據存儲資料固有論匙（ex.Kcon）用以生成存儲資料號址論匙 Ksav。

A7  
B7

## 五、聲明說明 (224)

「無程式使用限制」且「有記錄再生器限制」時，係在步驟 S 7 8 7 中，將記錄再生器固有繪點 (Kdev) 作為存儲資料繪點號碼 Ksav，或記錄再生器固有繪點 (Ksav) 用以生成存儲資料繪點號碼 Ksav，或，另外，保存於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著。與其他繪點別列的映號繪點做為存儲資料繪點號碼 Ksav 使用也可。

「無程式使用限制」且「無記錄再生器限制」時，係在步驟 S 7 8 7 中，系統共同繪點，譬如將系統筆名繪點 Keys 作為存儲資料繪點號碼 Ksav，或根據系統筆名繪點 Keys 用以生成存儲資料繪點號碼 Ksav，或，另外，保存於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著。與其他繪點別列的映號繪點做為存儲資料繪點號碼 Ksav 使用也可。

在步驟 S 7 8 9，係在步驟 S 7 8 5 ~ S 7 8 8 其中之一階段由被生成後之存儲資料繪點號碼 Ksav 便存儲在被容納於記錄再生器。

當西，在步驟 S 7 9 0，在步驟 S 7 8 2、S 7 8 3 中使用最後之限制資訊被使用者的資料管理檔案，資料管理檔案，譬如如形成圖 8 1 所示之構成，做為項目係合資料管理，於各信息識別子，記錄再生器識別子，程式使用限制，記錄再生器限制。

圖 8 2，係存圖 8 0 之造形用以再生，執行結果的於記錄再生器之後存儲實物或經資訊，而在步驟 S 7 9 1，係用以圖出執行程式之存儲資料識別子，記錄再生器識別子。

A4紙張及適用中國國家標準 (CNGB44) 規格 (210×297 公厘) - 227-

A7  
B7

## 五、聲明說明 (225)

Kdev) 用以生成存儲資料繪點號碼 Ksav，或，另外，保存於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著。與其他繪點別列的映號繪點做為存儲資料繪點號碼 Ksav 使用也可。並謂「無程式使用限制」且「無記錄再生器限制」時，係在步驟 S 7 9 0 中，系統共同繪點，譬如將系統筆名繪點 Keys 作為存儲資料繪點號碼 Ksav，或根據系統筆名繪點 Keys 用以生成存儲資料繪點號碼 Ksav，或，另外，保存於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著。與其他繪點別列的映號繪點做為存儲資料繪點號碼 Ksav 使用也可。

此等之導向化使能生成功能，係被運用對應於精简化繪點生成處理之底程算法，根據同一之存儲信息固有繪點，記錄再生器固有繪點並被之後之資訊，係依據同一之存儲信息固有繪點，記錄再生器固有繪點藉由被生成之詳略繪點形成可詳略被應用譯為精化繪點生成算法。

在步驟 S 8 0 0，係在上述步驟 S 7 9 6 ~ 7 9 9 其中之一使用被生成後之存儲資料譯碼化繪點被執行譯碼處理，並使譯碼存儲實物再生器 3 0 0 中被再生，執行。

云依據圖 8 0、8 2 中所示之存儲資料帶領，再生處理流程，則被形成「進行記錄再生器限制」之選擇的存儲資料依據存儲信息固有繪點因為被執行精化繪點，譯码化處理，所以持有同一存儲信息固有繪點並使用存儲信息固有繪點進行詳略形成可進行利用。又，被形成「進行記錄再生器限制」之選擇的存儲資料，係藉由記錄再生器識別子。

A4紙張及適用中國國家標準 (CNGB44) 規格 (210×297 公厘) - 229-

A7  
B7

## 五、聲明說明 (226)

子，步驟 S 7 9 1 中，由圖 8 1 所示資料管理檔案用以讓出存儲信息識別子，記錄再生器識別子，程式使用限制，記錄再生器限制資訊，該情形，使程式使用限制以「做」使記錄再生器識別子不一致時，或假記錄再生器限制資訊以「做」使記錄再生器識別子不一致時，則進行終了處理。

其次，在步驟 S 7 9 3、S 7 9 4、S 7 9 5，係根據資料管理檔案之記錄資料將該映號繪點生成資訊設定於步驟 S 7 9 6 ~ S 7 9 9 之 4 步驟其中之一。

「有程式使用限制」且「有記錄再生器限制」時，係在步驟 S 7 9 6 中，根據存儲信息固有繪點 (ex-Keon)，及記錄再生器固有繪點 (Kdev) 雙方被生成存儲資料繪點號碼 Ksav，或，另外，保存於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著，與其他繪點別列的映號繪點做為存儲資料繪點號碼 Ksav 使用也可。「有程式使用限制」且「無記錄再生器限制」時，係在步驟 S 7 9 7 中，將存儲信息固有繪點 (ex-Keon) 作為存儲資料繪點號碼 Ksav，或根據存儲資料繪點號碼 Ksav 用以生成存儲資料繪點號碼 Ksav，或，另外，保存於記錄再生器 3 0 0 之內部記憶體 3 0 7 內放著，與其他繪點別列的映號繪點做為存儲資料繪點號碼 Ksav 使用也可。

「無程式使用限制」且「有記錄再生器限制」時，係在步驟 S 7 9 8 中，將記錄再生器固有繪點 (Kdev) 作為存儲資料繪點號碼 Ksav，或根據記錄再生器固有繪點 (Kdev) 作為存儲資料繪點號碼 Ksav 使用也可。

A4紙張及適用中國國家標準 (CNGB44) 規格 (210×297 公厘) - 228-

A7  
B7

## 五、聲明說明 (227)

因為被執行號化，譯码化過程，所以持有同一記錄再生器識別子之記錄再生器，即藉由同一之記錄再生器進行譯碼形成可進行利程。因此，藉由存儲信息，記錄再生器號化形成可用以設定利用限制，該項可更提高存儲資料之安全性。

尚有，圖 8 0、圖 8 2 中，係顯示採用存儲信息固有繪點，記錄再生器固有繪點之存儲資料將其繪點，該詳述化的生成過程，但使用取代存儲信息固有繪點之存儲信息識別子，又取代記錄再生器固有繪點之記錄再生器識別子，譯码化過程由被認為執行存儲資料號化繪點，譯码化繪點之構成也可。

其次，依據圖 8 3 ~ 8 5 根據利用者之輸入的進行字對於用以生成存儲資料之號化繪點之詳略化構成，詳略化繪點之構成加以說明。

圖 8 3 係根據利用者之輸入的進行字用以生成存儲資料之號化繪點並差額於記錄裝置之處理流程。

步驟 S 8 2 1，係由存儲信息資料庫存儲信息識別子之處理，與前述過處環同様，步驟 S 8 2 2，係藉由利用者用以決定是否進行程式使用限制之選定的步驟，本構成中被設定之資料管理檔案，係猶如持有圖 8 4 所示之構成。

如圖 8 4 所示，資料，係含資料號碼，存儲信息識別子，記錄再生器識別子，前面藉由利用者之程式使用限制資訊。「藉由利用者之程式使用限制資訊」係用以設定要

A4紙張及適用中國國家標準 (CNGB44) 規格 (210×297 公厘) - 230-

AT  
BT五、發明說明（<sup>228</sup>）

不費用以判別使用者之利用者的項目。

在圖 8-3 中之成績流程之步驟 S 8-2-2 的使用限制並形成設定，則步驟 S 8-2-3 中被形成利用者進行字之輸入，該輸入，依舊如圖 8-2 所示由鍵盤等之輸入來直接輸入。

預錄入後之進行字，係在主 C P U 1 0 6，解剖語  
3 0 1 2 在限制下被輸出到記錄再生器 3 0 0-2，步驟  
S 8-2-4 中之成績，即根據輸入利用者進行字便存儲資料  
時數化論匙 Ksav 被生成，並為存儲資料時數化論匙 Ksav，  
係舊有而後進行字體做為論匙化論匙 Ksav 而可，或使用記  
錄再生器之生成匙。唯有存儲資料時數化論匙 Ksav 及 D E S  
(M K X - “進行字”進行生成也可)，將進行字做為輸  
入用以適用一方函數，並供錄出用以生成暗號化論匙

匙。步驟 S 8-2-2 中之利用者限制到 N=0 狀態時，則  
步驟 S 8-2-8 中，依據記錄再生器 3 0 0 之系統共同關係  
使存儲資料時數化論匙生成。

近而，在步驟 S 8-2-5 之後步驟 S 8-2-4，或步驟  
S 8-2-8 用生成之後之存儲資料時數化論匙 Ksav 並使存儲  
資料時數化論匙形成，步驟 S 8-2-6 中使用數化處理被  
形成之後之存儲資料被寄納於記錄裝置。

進而，步驟 S 8-2-7 中，在圖 8-4 之資料管理檔案以  
步驟 S 8-2-2 為由段落後之利用者從程式使用限制資訊，  
被寫入附屬於存儲信息識別子及記錄再生器識別子。

圖 8-5 係顯示藉由圖 8-3 之成績將各項約後之存儲資

AT  
BT五、發明說明（<sup>229</sup>）

藉之再生處理流程圖，一多路 S 8-3-1 中，由存儲信息資  
料運出存儲信息識別子，並在步驟 S 8-3-2 中由圖 8-4 所  
示之資料管理檔案演出存儲信息識別子，藉由利用常規方  
式使用限制資訊。

步驟 S 8-3-3 中，根據資料管理檔案中之資料用以執  
行判定，使「藉由利用常規方式使用限制」被設定時，  
則步驟 S 8-3-4 中，求出進行字輸入，步驟 S 8-3-5 中，  
根據輸入進行字用以生成暗號化論匙，該譯碼化論匙被成  
為成績，係被應用於檢驗化論匙生成處理之成績是否能  
被檢驗進行字被論匙化後之資料，須據圖 8-1 之進行字和  
由生成之後之譯碼化論匙形可詳論並設定於譯碼化論匙生  
成算法。

使步驟 S 8-3-3 之判定藉由利用者形成程式使用限制  
時，則步驟 S 8-3-7 中被容納於記錄再生器 3 0 0 之內部  
記憶體的系統共同關係，譬如使用系統名稱論匙 Ksys 並存  
儲資料時數化論匙 Ksav 被生成，或。另外，保存於記錄再生  
器 3 0 0 之內部記憶體 3 0 7 內存放著，與其他檢驗指標的  
論匙形可存儲資料時數化論匙 Ksav 使用也可。

在步驟 S 8-3-5，係步驟 S 8-3-5，步驟 S 8-3-7 其  
中之一中使用被生成之後之譯碼化論匙 Ksav 使被寄納於記錄  
再生之後之存儲資料之譯碼化論匙執行，並在步驟 S 8-3-6 之記  
錄再生器中被形成存儲資料之再生，執行。

藉依賴圖 8-3、8-5 中所示之存儲資料寄納，再生  
成績流程，則被形成「藉由利用者進行程式使用限制」之

AT  
BT五、發明說明（<sup>230</sup>）

進單的存儲資料係因為藉由模擬利用者輸入進行字的論匙  
被執行論匙化，譯碼化處理，所以進單入每一進行字時進  
行運算並可形成可利用，可成為提高存儲資料之安全度。

以上，對於無項之存儲資料內容的處理，再生處理狀態  
單了規模，僅將上述之成績進行點狀表示之處理，譬如使過  
行字，記錄再生器識別子，存儲信息識別子等任意組合進  
行使用以生成存儲資料時數化論匙，譯碼化論匙之情形  
也可。

## (17) 不正當複製之排除 (Revelation) 機制

如已經說明，本發明之資料處理過程中，由單置  
5 0 0 (參考圖 3)，進單度量 6 0 0 諸被提供之範圍的  
存儲資料在記錄再生器 3 0 0 中，用以執行認証，暗  
號化處理等，藉由寄納於記錄再生器之機制提高提供存儲信  
息之安全性，同時又，僅使正當利用者皆可利用之構成

。由上述之認明能這裡解，輸入存儲信息，藉由使用並構  
成於記錄再生器 3 0 0 之暗號或產生 3 0 2 并單納於內部  
記憶體 3 0 7 之機制的簽名論匙，主導匙，對舊生或新  
匙 (參照圖 1-8)，使認証處理，即論匙化處理，譯碼化處理  
被形成時，用以寄納該論匙資訊之內部記憶體 3 0 7，係  
如前圖 1-8 所示，基本上由構成由兩部皆有以取以存儲該  
的半導體晶片，其有多層構造，而其內部記憶體係被接於  
記憶等之底層，並被構成於最下層，又，使動作之電壓或

AT  
BT五、發明說明（<sup>231</sup>）

且頻率之寬頻率等，被構成做為外部難以不正當資料  
之譯出的特性為依據，但萬一內部記憶體之不正當採取  
被執行，使此等之機制與資訊等跳出，在未有正規許可證之  
記錄再生器被複製時，藉由複製之後之論匙資訊被不正當  
的存儲信息利用者可能被形成。

於此，由於此等之不正當複製藉由論匙之複製對於用  
以防止複製者之不正當利用的機制加以說明。

圖 8-6 係顯示藉以說明本構成「(17) 不正當複製  
之排除機制」方塊圖，記錄再生器 3 0 0，與前述圖 2、  
圖 3 所示記錄再生器同樣，具有內部記憶體，前並已說  
明 (圖 1-8) 各種之機器資料，前述，具有記錄再生器識  
別子，尚有，於此，係藉由第三者被複製之記錄再生器識  
別子，該資料等係不願被寄納於圖 3 所示內部記憶  
體 3 0 7，圖 8-6 所示記錄再生器 3 0 0 之機器資料等，係  
藉由單納或單納 3 0 2 (參考圖 2、3) 在可存取的記憶  
體彙整，並從行分割後為被認知之機制。

為了用以實現不正當複製之排除機制，被認為以記憶  
存儲信息資料後之外部部的不正當記錄再生器識別子名單  
如圖 8-6 所示，在存儲信息資料，係藉由不正當之  
記錄再生器識別子 (IDdev) 名單用以保有跡跡 (Reve  
lation) 名單，進而，原有該識別子之單納或拆分用之名  
單核對於 ICRev。不正當之記錄再生器識別子 (IDrev)  
名單，係使存儲信息提供者，或管理者，譬如由不正當複  
製之流動狀態轉判明後之不正當記錄再生器識別子 IDdev 並

43  
F9

## 五、聲明說明（<sup>232</sup>）

行名單化者，該排除名單係譬如前由配送總匙 Kdis 被暗號化並進行容納也可。藉由記錄再生器對於譯碼處理，係暫和與前兩圖 2-2 之在傳信員下載處理之無異現象。

當有，於此，爲了客易理據，將所列各名單做爲某獨之資料顯示於圖 8-6 之存儲信息資料中。但譬如在前面已引之存儲信息資料之擴展部的摘要裏是惟此方法（譬如參考圖 3-2～3-5）中半角符號存儲也。詳此情形，僅係由而前已說明之故。對第 I C V A 之存儲名單使理據方計資料之修改成對被形容。從某名單存儲的修改方面而言，僅係由存儲對第 A：I C V A 之存儲對被形容，並能記錄再生範內之核對值 A 成就地叫 I C V A 這項用，而不必要用以容納對其生成後的 I C V T C V 。

將拆散版做為單獨之資料並使其於存儲信息資料中時，  
藉由步驟之審核對照用名單核對值 ICVrev 以執行拆散之  
對照，同時由名單核對值 ICVrev 及存儲信息資料中之其他  
部分複核以生成中間核對值並做為進行中間核對值之  
驗證處理的構成。

藉由將之直接改用為單字典對值  $ICV_{ret}$  的排除名單之檢核方法，將原狀述圖 2-3、圖 2-4 已另以之  $ICV_A$ 、 $ICV_B$  等級別產生變成同樣之方法可執行。即，將保存於記錄再生障礙統計庫裡 3-0-2 之內部記憶體 3-0-7 後的後續產生備份成  $ICV_{ret}$ -raw 數為論述，並將合於存儲信息資料之辨名存為偽名依據圖 2-3、圖 2-4 已說明之  $ICV$  實力算方法論，用以比較計算其篩選之結果。

本研究乃透過月牙湖調查標準 (CNS) A1 標準 (200 公里) - 235 -

N  
22

五、聲明與明 (234)

就處理等之前的步驟被執行。對於下載處理，係使用如該面圖 2 之說明，般為面圖 2 之處理流程的執行前步驟，或般為被攝入於面圖 2 之處理流程中的處理使該面圖 8 7 之處理前步驟。

能記錄再生器 300 億個網路等之通訊裝置接收存儲信息提供時，係用以確立與步驟 S 911 中之存儲信息配對的判斷指標。由於一進階選擇 S 912

在步驟 S 902，係存媒體包資料之集散部用以收存排除名單（參考圖 8-6）。該名單取得處理，係在媒體內有存儲信息時，則安裝 3 所示控制部 301 通過接收部 304 由該系統進行指出，而由訊息裝置有存儲信息時，則後收裝 3 所示控制部 301 通過訊息裝置 305 由存儲部意記取到步驟 904。

其次步驟 S 903 中，判別部 301，係在記錄再生器號碼是否在步驟 302 由基層 500 或資訊供應 600 處理後之拆解名單轉交到記錄再生器號碼處理部 302，並執行該部將碼底成識記。記錄再生器號碼 300，係在內部是否有聯絡依對碼生成地點 *Kcv-rev*，將接收後之拆解名單做為信息用以適用該地點依對碼產生底層 *Kcv-rev*，實如依據圖 2.3、圖 2.4 等已說明之 *I CV = r rev* 之方法用以計算其算得值 *I CV = r rev*，並用以比較計算結果及被容纳於存儲器之資料之無誤 (Header) 內的核對值：*I CV = r rev*，在進行一一致後即刻判定無異狀 (步驟 S 904 Yes)，來一致時，則判定有異狀，並返還步驟 S 909

本的張氏在適用中國語文標準 (CNS) A4 規格 (210 x 297 毫米) - 237 -

A7  
B7

### 五、發明說明(233)

值 I C V - r e v " 及被容納於集管《 Header 》內後之核對值： I C V - r e v ，在進行一致後時，則進行判定并當改

含名原核對值 ICVrev 之中阅读對值，參見如，如圖 2-5 所示，將被保存於記錄再生器結構或處理部 3-0-2 之內部記錄體 3-0-7 的總級對值生成值 Kevt 做為論點，並在記錄延後之 Header 內之核對值 A，核對值 B，名原核對值 ICVrev，並再根據格式加上存取信息級對值後之信息存用以備用更正其値已說明之 ICV 計算方法進行生成。

此等之拆除名單，名單板對應，係造就 D V D 、 C D 等之媒體 500 套。資訊硬盤 6000 套，或資訊記錄卡等之記錄裝置 4000 套並被提供到記錄再生器 3000 套。於此記錄再生器 3000 套，係由正當的論點之記錄再生器時，則會有被不正當複製之識別子 ID 的情形。

圖 8-7 及圖 8-8 係顯示如此構成中之不正當的記錄再生器之消除或處理流程圖。圖 8-7 係由 D V D 、 C D 等之歷程 5 0 0 、或選購裝置 6 0 0 0 提供存儲信息時之不正當記錄再生者藉助「 Revocation 」處理流程圖，圖 8-8 係由記錄卡等之記錄裝置 4 0 0 提供存儲信息時之不正當記錄再生者藉助「 Revocation 」處理流程圖。

首先，對於擴 87 之處理流程加以說明。步驟 S 901，係用以備存媒體、存儲信息之提供，即進行再生處理或下車要求的步驟。該圖 87 所示之處理，係曾如右記般再生應用以備存 D.V.D 磁盤並供應用以執行下

名譽冊及名譽冊士哥羅正傳集 (CNS) MM 權集 (200 + 207 公集) - 230 -

A7

五、聲明說明 (235)

做為處理結果為行格了此處。  
其次，步驟 S 905 中，記錄再生器階級處理部  
302 和控制部 306，係將再生器階級處理部  
302 之增加／降低化部 308 徒變對 I C V T 之  
計算，選取對 I C V T 一係，係將 25 所示，將被保存  
於記憶體中再生器階級處理部 302 之內部機制 307 的系統  
資訊名稱為 Keys 係後端論點。將中間板對信以 D E S 進行化  
並產生成一塊，有各部分對數值，係將 I C V A。  
I C V A 之驅動規則，係在該圖 8 7 行為處理過程中低  
階者，但目前而已故明之圖 39 ～圖 45 之邏輯及流程同樣

其次，步驟 S 9 0 6 中，用以比較生成後之總核對值 I C V t 及參照《 Header 》內之 I C V t，在進行一致後時（在步驟 S 9 0 6 Yes），則進到步驟 S 9 0 7。未一致時，則被判定至重複，並進到步驟 S 9 0 9 略為

如前面已說明，核根對值  $ICV_t$ ，係  $ICVa$ 、 $ICVb$ 、進面，根據資料格式之各存儲信息區段的核對碼等，將被合於存儲資訊資料之部分對值來尋找行徑，但從此，在此等之部分對值後進面，將排除名單之更改點到用單字類別  $ICVr$ ，除各部分相對值之外，以用驗此等全部之更改，藉由上述處理後所生成之後核根對值與被容納於集首（Header）內之核對值： $ICV_t$  進行一致後，則判斷  $ICVa$ 、 $ICVb$ ，各存無信息區段之

**五、發明說明 (238)**

核對號，及名單核對號 ICRev 全部無異議。

並而到步驟 S 9 0 7 時，係將形成可用以比較判定無異議之後之記錄名單，及被容納於自己之記錄再生器 3 0 0 後之記錄再生器識別子 (IDev)。

由存儲信息資料在被譯出後之不正常的記錄再生器識別子 IDev 之名單被含有自己之記錄再生器的識別子 IDev 時，則該記錄再生器 3 0 0，係將判定具有不正確複製之記錄資料，並進到步驟 S 9 0 8，以後之步驟中止。譬如說不執行步驟 S 9 0 8 後之步驟再生器中止。

步驟 S 9 0 7 中，在不正常之記錄再生器識別子 IDev 之名單被判定來含有自己之記錄再生器的識別子

IDev 時，則該記錄再生器 3 0 0，係將判定具有正當的錄製資料，並進到步驟 S 9 0 8，以後之步驟，譬如，程式執行處理，或形成可執行步驟 S 9 2 2 之存儲信息下載處理等。

第 8 9 8 係顯示用以再生非類於記憶卡等之記錄資訊 4 0 0 之存儲信息資料時，如前所說已記憶卡等之記錄卡等之記錄識別子 4 0 0 及記錄再生器 3 0 0，係將圖 2 0 步驟之互換區域處理 (步驟 S 9 2 1) 被執行，步驟 S 9 2 2 中，僅在相互認證 OK 時，進到步驟 S 9 2 3 以後之處理，相互通訊失敗時，則形成步驟 S 9 3 0 之錄製，以後之處理不被執行。

在步驟 S 9 2 3，係存儲信息資料之焦點都用以取得辨別名單 (參看圖 8 8)，以後步驟 S 9 2 4～

**五、發明說明 (237)**

S 9 3 0 之處理，係存儲圖 8 7 中之對應處理同樣之處理，即，藉由名單核對號之名單驗證 (S 9 2 4、S 9 2 5)，藉由紀錄對照之驗證 (S 9 2 6、S 9 2 7)，用以執行比較 (S 9 2 8) 名單之項目及自己之記錄再生器識別子 IDev，並由存儲信息資料在被譯出後之不正常的記錄再生器識別子 IDev 之名單被含有自己之記錄再生器識別子 IDev 時，則該記錄再生器 3 0 0，係將判定具有不正確複製之後之記錄資料，並進到步驟 S 9 3 0，進到此以後之步驟，譬如說為不能執行步驟 S 9 3 0 所示之再生處理。另外，在不正常之記錄再生器識別子 IDev 之名單被判定來含有自己之記錄再生器識別子 IDev 時，則該記錄再生器 3 0 0，形成判定具有正當之論點資料，並進到步驟 S 9 2 9，形成可供執行以後之手續。

如此，本說明文之資料處理裝置中，係存儲信息提供者，或管理者提供之存儲信息一起用以識別不正常的記錄再生器之資料，而在不正常之記錄再生器識別子 IDev 進行名單化或將辨別名單為存儲信息資料之產生器的稱呼資料並一起提供到存儲信息利用者，而記錄再生器使用者，係藉由記錄再生器在存儲信息利用的用之前，用以執行核對被容納於自己之記錄再生器的記錄再生器識別子 IDev，及名單之記錄識別子並使進行一級之實存存取，而作為不使執行以後之處理所以用以複製論點資料並藉由容納於記錄識別子之後之不正常的記錄再生器形成可用以排除存儲信息利用。

**五、發明說明 (238)****(1) 安全晶片構成及製造方法**

如前所述已說明，記錄再生器總體處理部 3 0 2 之內部記憶體 3 0 7，及記憶體 4 0 0 之內部記憶體 4 0 5，因兩者均以保持存儲器等之直讀式資料，所以由外部有必然形式數點以不正確譯出之構造，因此，記錄再生器總體處理部 3 0 2，記錄後置研磨區 4 0 1，係當如被認為外接持存點以直取存儲的半導體晶片，具有多層構造，而其內部之記憶體係被持接於最層之最層，或被構成於最下層，又，使動作之覆蓋或直取率之直取率等，並構成欲與所持存點記憶體具有由外接持存點以不正確資料譯出的特性。

可是，在上述之說明所能推測，譬如說在無再生器總體處理部 3 0 2 之內部記憶體 3 0 7 在於記錄再生器識別子 IDev 等之記錄再生器形成必需要寫入不同的資料，又，晶片內之非易失性的記錄領域，譬如說在閃光記憶體、F e R A M 等各晶片之初期資訊，譬如寫入選項資訊 (I D) 或狀態監聽資訊後，譬如在晶片上寫入所持存資料之再插入，進而必要形成因由。

譬如說將之寫入資料的譯出，為將其寫入處理器為具圖面之方法，係當如將資料寫入之指令由訊通協議傳為秘密，或，將資料晶片上之資料寫入指令的並號碼，及在秘品化之後用以分離被利用活用的信號碼之構成，在基板上之晶片不直接送信號為限使資料寫入指令不會形成有效等之

**五、發明說明 (239)**

方法。

可是，即使採用如此之譬如技術方法，但對於具有記憶元件之專門知識者而言，若非使電路驅動之技術之技術，則對晶片之資料寫入領域可借由輸出，又，如使資料寫入之指令循訊協議傳為秘密，但這訊協議之部份可能經常存在。

如此，採用以保持秘密資料之可改變的地址處理資料之容納元件作此通過，係形成威脅而虧處理系統全體的結果，又，為了用以前述方式之譯出，也可做為不實質資料譯出指令自體之構成，如該情形，即使用以執行正當之資料寫入時，對記憶體之資料寫入用以確認是否實際進行，即使被寫入之後之資料那樣不能用以判斷是否正確進行，僅便進行不良資料寫入之品項可能產生被供給。

有鑑於此之實質原因，於此，提供一種安全晶片構成及安全晶片寫入方法，在 F e R A M 等非易失性記憶體做為可正確之資料寫入，同時將資料之譯出形成因由。

圖 8 9 係示資料寫入所適用的前述之記錄再生器總體處理部 3 0 2 或記憶體 4 0 0 之轉換處理部 4 0 1 的安全晶片構成，圖 8 9 (A) 係顯示晶片之製造過程，即資料之寫入過程中之安全晶片構成，圖 8 9 (B) 係示晶片以寫入資料之後之安全晶片的製品構成，譬如記錄再生器 3 0 0，記錄裝置 4 0 0 之例。

製造過程中之安全晶片，係在處理部 3 0 0 1 安裝型固定用信號號 3 0 0 3，及各個指令信號號 3 0 0 4 被灌

A7

B7

**五、發明說明 (242)**

接，或理部 8 0 0 1，係以被指用信號線 8 0 0 3 被設定後之模式，暫和根據資料寫入模式之資料譜出模式對非易失性記憶體之記憶部 8 0 0 2 的資料寫入處理，或由記憶部 8 0 0 2 用以執行資料譜出處理。

另外，圖 8 9 (B) 之安全晶片所製品中，係使安全晶片與外部連接接口，用達機器，其餘元件等以訊用信號被接通，但模式信號線 8 0 0 3，係呈非灌滿狀態，具異性的處理，僅當如將模式指用信號線 8 0 0 3 進行灌滿測試，吊於 V ccc，用以切斷該信號，或以紙條遮擋指甲外封等。藉由如此處理，製品出貨後，係對安全晶片之模式信號線被存取形或復原，由外部晶片之資料進行譜出或寫入可提高困難性。

追而，本構成之安全晶片 8 0 0 0，係有對資料之記憶部 8 0 0 2 寫入處理，及撰寫於記憶部 8 0 0 2 之後之資料譜出處理形因循之構成，即便使第三者在模式信號 8 0 0 3 之存取進行成功時也可防止不正常的資料寫入，譜出。圖 8 9 所顯示具有本構成之安全晶片中之資料寫入或譜出流程視圖。

步驟 5 9 5 1，係將模式信號線 8 0 0 3 設定成資料寫入模式或資料譜出模式的步驟。

步驟 5 9 5 2，係由晶片取出認證用資訊的步驟，本構成之安全晶片，係當並非由電纜 (Wire)，屏版 ROM 構成，預先在選行、驗證技術中之認證用的鑑匙資訊等，在認證處理被需要必要的資訊，步驟 5 9 5 2，係用以

A7

B7

**五、發明說明 (242)**

其次，追而，圖 9 1 係顯示並為安全性之元件構成的實施例圖。在該例，係使安全晶片之記憶部 8 2 0 0 為部分之 2 個領域，一方區域可實質性寫入於併用領域 (R/W: Read Write 領域) 8 2 0 1，而他方僅僅可資料寫入之寫入專用領域 (W/O: Write Only 領域) 8 2 0 2。

構成中，在寫入專用領域 (W/O: Write Only 領域) 8 2 0 2，係寫入資訊被限制，諸號子資料等要求高安全性之資料，而一方之安全性較選擇而高，譬如將核對用之資料等寫入譜出寫入併用領域 (R/W: Read Write 領域) 8 2 0 1。

處理部 8 0 0 1，係由譜出寫入併用領域 (R/W: Read Write 領域) 8 2 0 1 之資料譜出處理，係維持前述之圖 9 1 之說明之認證處理用以執行資料譜出處理。可是，資料寫入處理，係依據圖 9 2 之次序進行執行。

圖 9 2 之步驟 S 9 6 1，係將模式信號線 8 0 0 3 設定成寫入模式之步驟，在步驟 S 9 6 2，係用以執行保護範圍 8 0 0 1 已說明和諒的認證處理，在認證處理形或復原，並進到步驟 S 9 6 3，進階指令信號線 8 0 0 4，在寫入專用 (W/O) 領域 8 2 0 2 第一項安全性高的鑑匙資料等資訊，在譜出寫入併用領域 (R/W: Read Write 領域) 8 2 0 1 係安全性強度來的，譬如將核對用資料寫入指令對應部 8 0 0 1 進行輸出。

在步驟 S 9 6 4 係按接受指令後之處理部 8 0 0 1，將根據危險之資料寫入處理分別對寫入專用 (W/O) 領域

A7

B7

**五、發明說明 (243)**

讓出該認證資訊並用以執行認證處理，譬如將正規的資料寫入識別，資料譜出暨選擇對訊用信號線用以執行認證處理，則被取得認證 OK (步驟 5 9 5 3 中之 Y es) 之結果，但若不正確的資料寫入型態，資料譜出並選擇接於訊用信號線用以執行認證處理時，則認證失敗 (步驟 5 9 5 3 中之 N o)，並在該時點使處理被中止，認證或運，係當如依據前述已說明之圖 1 3 的相互認證處理手續可執行。圖 8 9 所示之處理部 8 0 0 1，係只有其執行此等之認證處理的構成，此係，譬如群由開前指出說明之圖 2 9 所示被嵌入於記憶部 4 0 0 之等級或處理部 4 0 1 的控制部 4 0 3 之後之命令寄存器各同樣之構成可實現。譬如圖 8 9 之晶片處理部，係存有與圖 2 9 所示被嵌入於記錄裝置 4 0 0 之等級或處理部 4 0 1 的控制部 4 0 3 後之指令寄存器同樣之構成，並被選擇於各匯總令指號線 8 0 0 4 後之機器被指定之指令 N o 被輸入，則用以執行對應之處理，並可形成用於執行認證處理程序。

處理部 8 0 0 1 係於認證處理中僅形成或既時，接受資料之寫入命令，寫資料之譜出指令用以執行資料之寫入處理 (步驟 S 9 5 5)，或資料之譜出處理 (步驟 S 9 5 6)。

如此本構成之安全晶片中，係在資料之寫入時，譜出時被用以執行認證處理的構成，所以由於尚未有正規權利之第三者由安全晶片之記憶部可用以防止資料之譜出，或寫入到記憶部。

本說明大意適用中國國家標準 (CH5144 條例 (210+297 份量)) - 244 -

A7

B7

**五、發明說明 (243)**

8 2 0 2，譜出寫入併用領域 (R.W: Read Write 領域) 8 2 0 1 進行執行。

又，圖 9 3 係顯示被寫入於寫入專用 (W/O) 領域 8 2 0 1 後之資料的驗證或復原圖。

圖 9 3 之步驟 S 9 7 1，係處理部 8 0 0 1 中，根據被寫入於寫入專用 (W/O) 領域 8 2 0 2 後之資料使用認證處理執行。此之執行構成，係當讀出之記錄或處理執行構成同樣，將被存於於指令寄存器後之等級或處理程序由進行新序執行之構成被實現。又，處理部中之被執行的暗號處理算法係由將被設定，譬如可被用以執行前面已說明之 D E S 算法的構成。

其次，在步驟 S 9 7 2，則被選擇於安全晶片後之驗證或復原處理部 8 0 0 1 用以接收複製複原結果，接著，步驟 S 9 7 3 中，在解述記憶部對進行寫入處理後之正確的寫入資料在處理部 8 0 0 1 中被執行之算式及適用同樣之暗號化處理取得之結果，由處理部 8 0 0 1 用以比較暗號化結果。

使比較之後結果若有一同，則被寫入於寫入專用 (W/O) 8 2 0 2 後之資料被驗證或正確。

在該構成，係當認證或復原被破壞或被誤用而將同一形式可執行，則被可識出底層，係被限定於寫入併用領域 (R/W: Read Write 領域) 8 2 0 1，而被寫入於寫入專用 (W/O) 領域 8 2 0 2 後之資料譜出，係不可能，並而形成高的安全性之構成。又，與元組後為不能譜出之

本說明大意適用中國國家標準 (CH5144 條例 (210+297 份量)) - 245 -

## 五、發明說明（<sup>244</sup>）

晶片不同，被構成有讀出寫入併用領域（R/W：Read Write）或僅存儲（S：Storage）之區塊。

以上，一方面參考肯定之實例，一方面對於本發明做了詳評。可是，在不脫離本發明之主旨的範圍內著者不能直接或用該實例而係自如其言，即，在所解釋之形態將本發明做了揭示，所以不應單定性的被解釋。又，在上述之實例與所傳存傳信息之記錄，可將之記述再者並非爲了說明，但僅可資料記錄，僅可資料性之裝置中也可適用本發明之構成，本發明係個人電腦、遊戲機器、一些其他各種機器或處理器中可實現，爲了用以判斷本發明之主旨，應參考記載於後之專利申請範例。

【黎明之效果】

如此，若依據本證明之資料來規範釐定及資料處理方法，則將存儲信息資料分割成數個部分後之部分資料對合時，上以部分資料集合做為核對值，但由於是由該部分之部分資料處理而以執行部分資料之驗證處理，並將部分資料對合後數個部分資料合後之部分資料對合無須進行驗證函由部分資料對合後使用所用核對之核對處理，對應於以備得部分資料對合後數個部分資料對合無須之部分資料集合無需應用以執行驗證處理做為構成，所以對於存儲信息資料主體與試算子之一核對值之構成不同，形成可分性的驗證處理，又，全體之驗證處理，也使用部分資料對合進行執行，所以形態有別。

布热津斯基谈中国民主精英 [CNESAM 版本 (200 x 237 页)] - 217 -

五、婚姻法附录(245)

進而，若依據本發明之資料處理装置及資料處理方法，則對無寫改之處的資料部分用以告別檢測處理等，存儲信息資料之使用狀態，譬如根據下載量、再生處理形成可驗證處理，可進行依據使用狀態之有效的驗証。

進而，若從日本發明之資料處理装置及資料處理方法，則爲了用以執行資料編號化、資料譯碼化、資料壓縮化、資料處理或、資料傳輸等之稱號，須度量成形必要的個別編號而不需音譜於記憶體，爲了用以生成此等之個別編號者有主論述者歸屬於記憶體之擴張，使資料處理或之自組運算器，始能將其資料譯碼等之個別編號獲得，持別對於此等之個別編號之主論述者由記憶體取出，再搬取後之主論述，及資料處理資料之識別資料，譬如用以執行運用 D E S 算法之暗號處理，做爲用以生成暗號資料，認證資料等之個別編號之識別，所以假使個別編號由記憶體不被改變，爲了取得識別號此，依個別編號生成算式，及生識別之雙方資訊，進而裝置或資料之識別資料等，便度量之資訊成形必要，成爲可能藉高階資料處理系統之安全性，又使個別編號的識別在何理由混淆時，其被識別裝置因應被限制於個別編號之範圍，所以可說對系統名稱無關係

然而，若依據本發明之資料處理裝置及資料處理方法，則根據裝置或資料之識別資料，用以逐次生成個別鑰匙，所以將適用於各自之裝置的鑰匙名單在管理裝置不必加以保持，形成堆疊安全元件及降低由來最系統資源。

中国科学院植物研究所植物学集刊 (CHINESE JOURNAL OF BOTANY) 2002, 20(2): 241-242

13  
BY

## 五、聲明說明(246)

當而，若依據本發明之資訊處理閘置，資料處理方法及存儲信息資料源或方法，則在存儲信息資料源用以容納不正確機器名單之別號與資訊，並在記錄再生過程中之存儲信息利用之前，用以執行不正確機器，及啟動利用存儲信息之記錄再生過程的記錄再生此循環步驟之執行或處理，致達到結果，在合於不正確機器名單之循環步驟再生此循環步驟使執行一循環步驟存目時，則以之後為底，實即如循環步驟中以止存儲信息資料源而為，下級，再生此循環步驟之執行的梯度所以看由不正確機器後之再生循環等步驟可用以排除存儲信息的不正確資料。

進而，若欲據本發明之資料而推廣擴展，資料處理方法及存儲信息資料生成方法，則應為擁有保存信息資料中之不正確姓名單用以核對個合於存儲信息資料之構成，所以可達成防止不單名自證之篡改，進而成為可提供高安全性的存儲信息資料利用構成。

而後，若依據本發明之資料處理裝置及資料處理方法，則在記錄再生器、P-C 及資料處理裝置用以各納資料處理裝置固有之操作因有據此，其在用以利用存儲信資資料之其他資料處理裝置用以將各不同系統傳輸此所以根據存儲信息之利用限制形成可存儲信息處理、資料處理裝置、擴充此等傳輸依據存儲信息之利用限制以選擇性地加以利用，譬如當在該資料處理裝置中有可利用之存儲信息時，則使用資料處理裝置從存儲中取。另外，在其餘之系統中也有可利用存儲信息時用以安排其統共論據化執行存儲

本報係長度為廣之圖書之總集 (CNS) 之總集 (210 x 287 公釐) - 242 -

五、盛賜姐姐(247)

信息資料之核對並生成、核對處理。僅在進行核對成立時用以驅動電子化資料形成可進行再生，所以僅使該資料處理裝置可利用存儲信息，或在系統進行共同可利用之存儲信息等，形成可根據存儲信息之利用驅動的處理。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料驗證賦予方法，則以存儲信息區段單位可驗證，同時存儲信息資料之笨用態樣，當如可形成根據下繼處理、再生處理之間階化的驗證處理，可進行依據使用範圍之各項的檢驗。

進而，本發明之資料處理模塊，存儲信息資料生成方法，及資料處理方法中，係在存儲信息資料中設有枚數之存儲信息區段，在各存儲信息區段首位均設有能帶指稱存儲此區段、又轉換於存儲信息增強化之鍵點而進行增強化做為諮詢於集羣部之標識，所以單以復數之存儲信息區段存在，並使得資訊處理之必要的區段，及不要的區段進行配比時，也可形成為應用以連結各區段後之任意的資料構成。

本刊所用之数据由国家统计局、GDP核算小组提供。—编者注

## 五、發明說明 (240)

述而，若依據本發明之資料處理裝置，資料處理系統及資料處理方法，則將存儲信息資料之構成或持用為兩期性的構成，譬如持有一津之資料易於其構成，或藉由做為以交替用以形成單純化過程及非複雜化（平譯文）兩段之構成，形成可快速運用以執行其譯碼處理，根據存儲信息資料之內容的需要，譬如可形成適用於音質資料之再生等的頻繁化存儲信息資料之提供。

進而，本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，係使存儲信息資料可有效用以執行並應用後之聲音資料，或有圖像資料等情形之再生處理。即，將存儲信息資料之構成做為結合兩期資料及作伸長處理程式之情況，在再生處理裝置中，辦法可適用附帶的應用存儲信息資料之再生處理程式的伸長處理，在再生處理裝置內使用伸長處理程式不存取於回路不能再生之狀態。

述而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，則將存儲信息資料之構成做為以交替用以形成單純化過程及非複雜化過程，並將存儲信息資料藉由用以容納伸長處理程式及伸長程式運算後做為來源部之組合，使再生處理裝置可適用於應用存儲信息資料的伸長過程式根據無失真原則進行對應，進而使再生處理裝置可存取之記錄裝置等用以被共同適用的程式做為以執行伸長處理之構成，所以藉由利用非形不必用以執行程式來達處理，可形成有效的再生處理。

## 五、發明說明 (249)

## 【圖式之簡單說明】

圖 1 係顯示本發明之資料處理系統的構成圖。

圖 2 係顯示本發明被適用資料處理裝置之構成圖。

圖 3 係顯示本發明被適用資料處理裝置之構成圖。

圖 4 係顯示在基座上，資訊路上之存儲信息資料的資料格式圖。

圖 5 係顯示被合於存儲信息資料中之風管的處理力計圖。

圖 6 係顯示合於存儲信息資料中之區段資訊圖。

圖 7 係顯示使用 DES 之電子署名生成方法圖。

圖 8 係顯示使用三倍 DES 之電子署名生成方法圖。

圖 9 係用以說明三倍 DES 之處理圖。

圖 10 係顯示在一部分使用三倍 DES 之電子署名生成方法圖。

圖 11 係顯示電子署名生成中之處理流程圖。

圖 12 係顯示電子署名生成中之處理流程圖。

圖 13 係用以說明使用對稱鑰匙技術之將互通証視之處理程序圖。

圖 14 係用以說明公鑰証視圖。

圖 15 係用以說明使用非對稱鑰匙技術之互通証視之處理程序圖。

圖 16 係顯示使用椭圓曲線加法之階級化處理的處理流程圖。

## 五、發明說明 (250)

圖 1.7 係顯示使用轉圈由鍵相位之譯碼處理的處理流程圖。

圖 1.8 係顯示記錄再生器上之資料保持狀況圖。

圖 1.9 係顯示記錄裝置上之資料保持狀況圖。

圖 2.0 係顯示記錄再生器及記錄裝置之相互認證處理流程圖。

圖 2.1 係顯示記錄再生器之主端點及記錄裝置之對應端點的關係圖。

圖 2.2 係顯示存儲信息之下載處理中的處理流程圖。

圖 2.3 係用以說明核對碼 I : C V a 之生成方法圖。

圖 2.4 係用以說明核對碼 B : I C V b 之生成方法圖。

圖 2.5 係用以說明總核對值，記錄再生器固有核對值之生成方法圖。

圖 2.6 係顯示被保存於記錄裝置之存儲信息資料的格式（利用啟動資訊 = 0）圖。

圖 2.7 係顯示被保存於記錄裝置之存儲信息資料的格式（利用啟動資訊 = 1）圖。

圖 2.8 係顯示在側信息之再生處理中的處理流程圖。

圖 2.9 係對於記錄裝置之指令執行方法說明圖。

圖 3.0 係對於記錄裝置中之存儲信息資料的處理之指令執行方法說明圖。

圖 3.1 係對於記錄裝置中之存儲信息再生處理的指令

## 五、發明說明 (251)

## 執行方法說明圖。

圖 3.2 係用以說明存儲信息資料格式之格式形態 0 的構成圖。

圖 3.3 係用以說明存儲信息資料格式之格式形態 1 的構成圖。

圖 3.4 係用以說明存儲信息資料格式之格式形態 2 的構成圖。

圖 3.5 係用以說明存儲信息資料格式之格式形態 3 的構成圖。

圖 3.6 係用以說明格式形態 0 中之存儲信息核對值 I C V i 的生成處理方法圖。

圖 3.7 係用以說明格式形態 1 中之存儲信息核對值 I C V i 的生成處理方法圖。

圖 3.8 係用以說明格式形態 2、3 中之核對值，記錄再生器固有核對值之生成處理方法圖。

圖 3.9 係顯示格式形態 0、1 中之存儲信息下載處理的處理流程圖。

圖 4.0 係顯示格式形態 2 中之存儲信息下載處理的處理流程圖。

圖 4.1 係顯示格式形態 3 中之存儲信息下載處理的處理流程圖。

圖 4.2 係顯示格式形態 0 中之存儲信息再生處理的處理流程圖。

圖 4.3 係顯示格式形態 1 中之存儲信息再生處理的處

A7  
B7

## 五、發明說明（252）

發送範例。

圖 4-4 係顯示格式形態 2 中之存儲信息再生處理的處理流程圖。

圖 4-5 係顯示格式形態 3 中之存儲信息再生處理的處理流程圖。

圖 4-6 係用以說明存儲信息生皮者，及存儲信息驗證者中之核對值的生成，驗正方法圖（其 1）。

圖 4-7 係用以說明存儲信息生皮者，及存儲信息驗證者中之核對值的生成，驗正方法圖（其 2）。

圖 4-8 係用以說明存儲信息生皮者，及存儲信息驗證者中之核對值的生成，驗正方法圖（其 3）。

圖 4-9 係對於使用主鍵匙將各種鑰匙以個別生成之方法說明。

圖 5-0 係顯示對於使用主鍵匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例 1）。

圖 5-1 係顯示對於使用主鍵匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例 2）。

圖 5-2 係用以說明藉由主鍵匙之分開使用，對於用以執行判定限制之構成圖。

圖 5-3 係顯示對於使用主鍵匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例 3）。

A7  
B7

## 五、發明說明（254）

圖。

圖 6-7 係顯示存儲信息之構成例（例 4）圖。

圖 6-8 係顯示存儲信息之構成例 4 中的再生處理流程圖。

圖 6-9 係用以說明對於存儲資料之生成，容納處理圖。

圖 6-10 係顯示關於存儲資料之容納處理例（例 1）的處理流程圖。

圖 6-11 係顯示關於存儲資料之容納，再生處理中被使用資料管理檔案構成（例 1）圖。

圖 6-12 係顯示關於存儲資料之再生處理例（例 1）的處理流程圖。

圖 6-13 係顯示關於存儲資料之容納處理例（例 2）的處理流程圖。

圖 6-14 係顯示關於存儲資料之再生處理例（例 2）的處理流程圖。

圖 6-15 係顯示關於存儲資料之容納處理例（例 3）的處理流程圖。

圖 6-16 係顯示關於存儲資料之容納處理例（例 3）的處理流程圖。

圖 6-17 係顯示關於存儲資料之容納處理例（例 4）的處理流程圖。

A7  
B7

## 五、發明說明（255）

圖 5-4 係顯示對於使用主鍵匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例 4）。

圖 5-5 係顯示對於使用主鍵匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖（例 5）。

圖 5-6 係顯示將適用三倍 DES 之密鑰鍛造此使用單 DES 算法進行容納處理流程圖。

圖 5-7 係顯示根據優先順位之存儲信息再生處理流程（例 1）圖。

圖 5-8 係顯示根據優先順位之存儲信息再生處理流程（例 2）圖。

圖 5-9 係顯示根據優先順位之存儲信息再生處理流程（例 3）圖。

圖 6-0 係用以說明對於用以執行存儲信息再生處理中之新規範的選擇（伴員）處理構成圖。

圖 6-1 係顯示存儲信息之構成例（例 1）圖。

圖 6-2 係顯示存儲信息之構成例 1 中的再生處理流程圖。

圖 6-3 係顯示存儲信息之構成例（例 2）圖。

圖 6-4 係顯示存儲信息之構成例 2 中的再生處理流程圖。

圖 6-5 係顯示存儲信息之構成例（例 3）圖。

圖 6-6 係顯示存儲信息之構成例 3 中的再生處理流程圖。

A7  
B7

## 五、發明說明（256）

圖 7-9 係顯示關於存儲資料之再生處理例（例 4）的處理流程圖。

圖 8-0 係顯示關於存儲資料之容納或退例（例 5）的處理流程圖。

圖 8-1 係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成（例 3）圖。

圖 8-2 係顯示關於存儲資料之再生處理例（例 5）的處理流程圖。

圖 8-3 係顯示關於存儲資料之容納處理例（例 6）的處理流程圖。

圖 8-4 係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成（例 4）圖。

圖 8-5 係顯示關於存儲資料之再生處理例（例 8）的處理流程圖。

圖 8-6 係用以說明存儲信息不正當利用者撤除（Revocation）構成圖。

圖 8-7 係顯示存儲信息不正當利用者撤除（Revocation）之處理流程（例 1）圖。

圖 8-8 係顯示存儲信息不正當利用者撤除（Revocation）之處理流程（例 2）圖。

圖 8-9 係用以說明安全晶片之構成（例 1）圖。

圖 9-0 係顯示安全晶片之製造方法中的處理流程圖。

圖 9-1 係用以說明安全晶片之構成（例 2）圖。

圖 9-2 係顯示安全晶片（例 2）中之資料為入處理中。

AT

BT

**五、發明說明 (256)**  
的處理流程圖。

圖 9-3 係顯示安圣品 (例 2) 中之寫入處理資料核對處理中的處理流程圖。

**【元件編號之說明】**

- 1 0 6 …主 C P U .
- 1 0 7 …R A M .
- 1 0 8 …R O M .
- 1 0 9 …A V 處理部 .
- 1 1 0 …輸入處理部 .
- 1 1 1 …P I O .
- 1 1 2 …S I O .
- 3 0 0 …記錄再生器 .
- 3 0 1 …控制部 .
- 3 0 2 …輸出處理部 .
- 3 0 3 …記錄夾層控制器 .
- 3 0 4 …讀取部 .
- 3 0 5 …通訊部 .
- 3 0 6 …控制部 .
- 3 0 7 …內部記憶體 .
- 3 0 8 …總管／複製系統 .
- 4 0 0 …記錄裝置 .
- 4 0 1 …帶號處理部 .
- 4 0 2 …外部記憶體 .

AT

BT

**五、發明說明 (257)**

- 4 0 3 …控制部 .
- 4 0 4 …通訊部 .
- 4 0 5 …內部記憶體 .
- 4 0 6 …總管／複製化部 .
- 4 0 7 …外部記憶體控制部 .

- 5 0 0 …總管 .
- 6 0 0 …通訊裝置 .
- 2 1 0 1 …2 1 0 2 、2 1 0 3 …記錄再生器 .
- 2 1 0 4 …2 1 0 5 、2 1 0 6 …記錄裝置 .
- 2 9 0 1 …指令號碼選擇器 .
- 2 9 0 2 …指令寄存器 .
- 2 9 0 3 、2 9 0 4 …認證標記 .
- 3 0 0 1 …備要部 .
- 3 0 0 2 …監視 .
- 3 0 9 0 …記憶體 .
- 3 0 9 1 …存取信息分析部 .
- 3 0 9 2 …資料記憶部 .
- 3 0 9 3 …程式記憶部 .
- 3 0 9 4 …處理件長處理部 .
- 7 7 0 1 …存取信息資料 .
- 7 7 0 2 …撤銷 (Revocation) .
- 7 7 0 3 …名單核附值 .
- 8 0 0 0 …安圣品 .
- 8 0 0 1 …認證碼 .

AT

BT

**五、發明說明 (258)**

- 8 0 0 2 …記憶體 .
- 8 0 0 3 …模式信號錄 .
- 8 0 0 4 …指令信號錄 .
- 8 2 0 1 …讀出寫入用信紙 .
- 8 2 0 2 …寫入專用信紙 .

AT

BT

**六、申請專利範圍**

1. 一種資料處理裝置，係藉由記憶裝置或資訊裝置進行被提供之存儲信息資料的處理，其特徵在於具有：  
暗號處理部，對前述存儲信息資料用以執行暗號處理；及：

控制部，對前述暗號或處理部用以執行控制；

而前述暗號或處理部，其構成係具有：

將存儲信息資料傳為複數部分後之部分資料對合上以上部分資料集合係用以核對值並用以生成部分核對值，並藉由該係用以生成之部分核對值對應對應用以執行前述各部分資料之驗證處理；而將前述各部分資料集合全體用以執行驗證處理。

2. 如申請專利範圍第 1 項所記載之資料處理裝置，其中前述部分核對值，係將形成核對對象之部分資料作為信息，並藉由用以傳為前述部分核對值在生成之後之稱號並被生成之值。

前面述之相關對值，係將形成核對對象之部分核對值集合資料列用以生成中間對值，並使用該生成後之中間核對值，對應於用以傳為前述部分核對值在生成之後之稱號並被生成之值。

而前述暗號處理部，其構成係具有用以存管前述部分核對值生成的值及前述鍵接對值生成的值。

3. 如申請專利範圍第 2 項所記載之資料處理裝置，

## 六、申請專利範圍

其中前述地點處理部，係具有惟數種類之部分核對值生成或確認其屬於生成之部分核對值。

4. 如申請專利範圍第 2 項所記載之資料處理裝置，其中前述地點處理部 DES 地址處理裝置，

而前述地點處理部，係具有可執行 DES 地址處理之機制。

5. 如申請專利範圍第 1 項所記載之資料處理裝置，其中前述部分核對值，係將形成核對對象之部分資料做為信息在 DES-CBC 模式中被生成或有資訊認符號（MAC）。

而前述中間核對值，係將形成核對對象之部分核對值集合並列級為信息在 DES-CBC 模式中被生成或有信息認符號（MAC），

而前述地點處理部，係具有藉由 DES-CBC 模式用以執行確認處理之構成。

6. 如申請專利範圍第 5 項所記載之資料處理裝置，其中前述前述地點處理部具有之 DES-CBC 模式的暗號處理模組，係僅在形成確認對象之信息的一部分被適用三倍的 DES 之情形者。

7. 如申請專利範圍第 1 項所記載之資料處理裝置，其中前述資料處理裝置，係具有署名論述。

而前述地點處理部，

係對於前述中間核對值借由前述名稱將後之類號或識別號生成之值作為資料驗證後為核對值並進行適用之

## 六、申請專利範圍

構成。

8. 如申請專利範圍第 7 項所記載之資料處理裝置，其中前述資料處理裝置，係做為匿名論述並具有不同複數之署名論述。

而前述地點處理部，

係具有根據前述存儲信息資料之利用限制選擇由前述不同複數之署名論述將選擇後之署名論述對前述中間核對值進行適用之結果應認為資料驗證為核對值之與或否。

9. 如申請專利範圍第 8 項所記載之資料處理裝置，其中前述資料處理裝置，係做為許述複數之署名論述，且具有用以執行資料驗證處理大同於系統之全實體的共同署名論述，及用以執行資料驗證處理之各個的裝置固有之裝置固有署名論述。

10. 如申請專利範圍第 1 項所記載之資料處理裝置，其中前述部分核對值，係含：無管部分核對值，對於用以構成資料之一部分之無管內部資料被生成 1 以上；及存儲信息核對值，對於用以構成資料之一部分的存儲信息區資料被生成 1 以上；

而前述地點處理部，其構成係具有對於前述無管內部之部分資料無合用以生成 1 以上之無管部分核對值並用以執行核對處理，而對於前述存儲信息內部之部分資料無合用以生成 1 以上之存儲信息核對值並用以執行核對處理，進而，根據被生成之後前述無管部分核對值及前述

## 六、申請專利範圍

存儲信息核對值全部用以生成編碼對值並藉由用以執行核對處理以執行資料驗證。

11. 如申請專利範圍第 1 項所記載之資料處理裝置，其中前述部分核對值，係含無管部分核對值，對於用以構成資料之一部分的無管內部資料被生成 1 以上。

而前述地點處理部，其構成係具有對於前述無管內部之部分資料無合用以生成 1 以上之無管部分核對值並用以執行核對處理，進而，用以構成被生成之後前述 1 以上的無管部分核對值及前述資料用以構成資料之部分根據由前述存儲信息區資料所構成資料用以生成編碼對值並藉由用以執行核對處理以執行資料驗證。

12. 如申請專利範圍第 1 項所記載之資料處理裝置，其中前述資料處理裝置，係前述。

具有記錄裝置用以存取前述地點處理部中之正確性驗證執行後的資訊。

13. 如申請專利範圍第 1-2 項所記載之資料處理裝置，其中前述資料處理裝置，係前述。

具有再生處理部在前述地點處理部中用以再生正確性驗證被執行後之資料。

14. 如申請專利範圍第 1 項所記載之資料處理裝置，其中前述資料處理裝置，係前述。

具有再生處理部在前述地點處理部中用以再生正確性驗證被執行後之資料。

## 六、申請專利範圍

15. 如申請專利範圍第 1-4 項所記載之資料處理裝置，其中前述資料處理裝置。

係在前述地點處理部中之部分核對值的核對處理中，在使核對未成立時，

而前述地點處理部，其構成係具有用以中止再生處理之構成者。

16. 如申請專利範圍第 1-4 項所記載之資料處理裝置，其中前述資料處理裝置。

係具有控制裝置在前述地點處理部中之部分核對值的核對處理中，藉由以執行資料之無管部分核對值的核對處理，並執行獨立部署部分核對值之核對後的資料轉送至前述再生處理部並做為可再生者。

17. 一種資料處理裝置，藉由記錄媒體或訊號媒體進行資料存儲之存儲信息資料的處理，其特徵在於具有：

前述地點處理部，其構成係具有：

使驗證對象資料具有唯數種類之部分核對值，藉由該唯數種類之部分核對值被存儲資料用以執行資料處理並採取該資料驗證結果資料藉由用以實施應用署名論述往之地點處理，用以生成正確性驗證對象資料之核對值。

18. 如申請專利範圍第 1-7 項所記載之資料處理裝置，其中前述資料處理裝置，係藉由前述唯數種類之資料之





## 六、申請專利範圍

而前述專利範圍之說明，係根據發容於前述記述部後之認證函所生成用主論點 Make，及前述外部直接裝置之識別子的外部直接裝置識別子用以執行增號處理，並用以生成藉益外部直接裝置之認證函之 Xake 的構成。

5.0 . 如申請專利範圍第 4~7 項所記載之資料處理系統，其中前述資料處理裝置，係對資料用以執行署名處理的資料處理裝置，

而前述記述部，係具有用以生成前述資料處理裝置之資料處理裝置署名識別子 Kdev 並用以容納署名識別子生成用主論點 MKdev。

而前述增號處理部，係根據發容於前述記述部之署名識別子生成用主論點 MKdev，及前述資料處理裝置之識別子的資料處理裝置識別子用以執行增號處理，並用以生成前述資料處理裝置之資料處理裝置署名識別子 Kdev 之構成。

5.1 . 如申請專利範圍第 4~7 項所記載之資料處理裝置，係將用以執行增號處理必要之別別識別子，根據前述主論點，及增號處理對象之簽署或資料之識別資料進行生成之別別識別子生成處理。

而前述增號處理對象之簽署或資料之識別資料至少一部分為數位信息，並將前述主論點作為增號識別子進行適用之明確處理者。

5.2 . 如申請專利範圍第 5~11 項所記載之資料處理裝置，其中前述資料處理裝置用以執行 D E S 某法之認證處理者。

## 六、申請專利範圍

子用以生成存儲信息資料配給識別子，並用以執行該存儲信息資料之辨識化處理的構成。

5.5 . 如申請專利範圍第 5~14 項所記載之資料處理系統，其中前述存儲信息資料配給識別子，係具有用以生成複數不同之配給識別子生成用主論點為丁以生成複數不同之存儲信息資料配給識別子，並根據該複數之配給識別子生成用主論點及前述存儲信息資料配給識別子用以生成複數不同之存儲信息資料配給識別子，藉由該生成之複數之配給識別子用以執行增號處理並用以生成複數不同之存儲信息資料。

而前述存儲信息資料配給識別子，係具有用以存儲信息資料後供後置之複數不同之配給識別子生成用主論點至少 1 個之配給識別子生成用主論點，使用自己所有之配給識別子生成用主論點及同樣配給識別子生成用主論點藉由生成之配給識別子將複數化存儲可識別之構成。

5.6 . 如申請專利範圍第 5~13 項所記載之資料處理系統，係在前述複數之資料處理裝置之各自，用以容納同一之存儲信息資料生成用主論點為丁用以生成適用於存儲信息資料之識別子生成之存儲信息識別子。

並在前述複數之資料處理裝置之 1 個資料處理裝置 A 中，根據前述存儲信息資料配給識別子生成用主論點，及該資料處理裝置 A 之識別裝置子藉由該存儲信息資料配給識別子用以記憶該存儲之存儲信息資料。

在不同資料處理裝置 B 中，根據前述同一之存儲信息資料生成用主論點，及前述資料處理裝置 A 之識別裝置子

## 六、申請專利範圍

5.3 . 一種資料處理系統，係由複數之資料處理裝置被構成之資料處理系統中，其特徵在於：

前述複數之資料處理裝置各自，具有共同之主論點為丁用以生成適用於資料檢驗化、資料轉換化、資料驗證、認證處理、署名處理至少其中之一的識別或處理之論點。

並使前述複數之資料處理裝置各自，具有相應前述主論點，及相應或處理對象之簽署或資料之識別資料用以生成執行前述增號處理必要的共同之別別識別子的構成。

5.4 . 如申請專利範圍第 5~13 項所記載之資料處理系統，其中前述複數之資料處理裝置，

係藉由提供存儲信息資料之存儲信息資料提供裝置，及進行利用存儲信息資料之存儲信息資料用以存儲並被構成

並從存儲信息資料提供裝置及存儲信息資料用以存儲之雙方，具備前述增號處理必要之別別識別子的前述存儲信息資料提供裝置及存儲信息資料用以存儲並被構成之資料的轉換處理為丁用以生成存儲信息資料提供裝置的構成。

而前述存儲信息資料提供裝置，係具有根據前述增號處理生用主論點，及提供存儲信息資料之識別子的存儲信息資料識別子用以生成存儲信息資料提供裝置，並用以執行該存儲信息資料之塔試化處理。

而前述存儲信息資料利用裝置，係根據前述增號處理裝置生成用主論點，及存儲信息資料之識別子的存儲信息資料

## 六、申請專利範圍

子用以生成存儲信息資料配給識別子，並用以執行該存儲信息資料之辨識化處理的構成。

5.5 . 如申請專利範圍第 5~14 項所記載之資料處理系統，其中前述存儲信息資料配給識別子，係具有用以生成複數不同之配給識別子生成用主論點為丁以生成複數不同之存儲信息資料配給識別子，並根據該複數之配給識別子生成用主論點及前述存儲信息資料配給識別子用以生成複數不同之存儲信息資料配給識別子，藉由該生成之複數之配給識別子用以執行增號處理並用以生成複數不同之存儲信息資料。

而前述存儲信息資料配給識別子，係具有用以存儲信息資料後供後置之複數不同之配給識別子生成用主論點至少 1 個之配給識別子生成用主論點，使用自己所有之配給識別子生成用主論點及同樣配給識別子生成用主論點藉由生成之配給識別子將複數化存儲可識別之構成。

5.6 . 如申請專利範圍第 5~13 項所記載之資料處理系統，係在前述複數之資料處理裝置之各自，用以容納同一之存儲信息資料之識別子生成之存儲信息識別子。

並在前述複數之資料處理裝置之 1 個資料處理裝置 A 中，根據前述存儲信息資料配給識別子生成用主論點，及該資料處理裝置 A 之識別裝置子藉由該存儲信息資料配給識別子用以記憶該存儲之存儲信息資料。

在不同資料處理裝置 B 中，根據前述同一之存儲信息資料生成用主論點，及前述資料處理裝置 A 之識別裝置子

## 六、申請專利範圍

用以生成存儲信息資料識別子，並根據該生成之存儲信息識別子，前述資料處理裝置 A 中用以執行存儲並於前述記述部後之增號處理信息資料之辨識化處理的構成。

5.7 . 如申請專利範圍第 5~13 項所記載之資料處理系統，其中前述複數之資料處理裝置，

係藉由由主論點，及形成該主論點之認證對象的副裝置被構成。

並前述主論點及副裝置之雙方，具有認證論點生成用主論點及副裝置用以認證論點之構成。

而前述副裝置，係具有根據前述增號處理裝置生成用主論點，及該副裝置之識別子的副裝置識別子用以生成認證論點並用以執行認證處理之構成。

而前述主論點，係根據前述認證論點生成用主論點，及該副裝置之識別子的副裝置識別子用以生成認證論點並用以執行認證處理之構成。

5.8 . 一種資料處理方法，用以執行資料檢驗化、資料轉換化、資料驗證、認證處理、署名處理至少其中一種指稱該項資料處理方法中，其特徵在於具有：

另用以執行增號處理論點之論點的主論點，及該論點對象之辨識或資料之識別資料生成之論點生成步驟；及

藉由該論點生成步驟根據前述增號處理論點用以執行增號處理之論點處理步驟。

## 六、中華專利範圍

法，在前述資料處理方法中執行執行的資料處理，係指選定或資訊媒體有獨特之辨識號碼。

而前述論點生成步驟，

係根據用以生成適用於前述資料之辨號處理的前述論點 Kd1is 之前述論點生成或用主論點 Mkd1s，及前述論點資料之識別資料的資料識別子用以執行辨號處理，並用以生成前述論點之辨號論點 Kd1is 之前述論點生成步驟。

而前述論點生成步驟，

係根據前述論點生成步驟中生成的前述論點 Kd1is 用以執行前述資料之辨號處理的步驟。

0.0. 如申請專利範圍第 5.8 項所記載之資料處理方法，其中前述資料處理方法中之辨號執行的資料處理，係形成辨號資料之辨對象或辨識的外部選擇装置之認證處理，

而前述論點生成步驟，係根據用以生成前述外部選擇裝置之認證論點 Kake 的認證論點生成或主論點 Mkak，及前述外部選擇裝置之識別資料的外部選擇裝置識別子用以執行辨號處理，並用以生成前述外部選擇裝置之認證論點 Kake 的認證論點生成步驟，

而前述論點生成步驟，係根據前述論點生成步驟中達成子項之認證論點 Kake 用以執行外部選擇裝置之認證處理的步驟。

0.1. 如申請專利範圍第 5.8 項所記載之資料處理方法，其中前述資料處理方法中之辨號執行的資料處理，係

本辦法規定之中國國家標準 (CNB) A4 尺寸 (210×297 毫米) - 279 -

## 六、中華專利範圍

對資料之署名處理。

而前述論點生成步驟，

係根據用以生成前述資料處理裝置之資料處理裝置署名論點 Kdav 的署名論點生成或用主論點 Mkdav，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行辨號處理，並用以生成前述資料處理裝置之資料處理裝置署名論點 Kdav 的署名論點生成步驟。

而前述項署名處理步驟，

係根據前述署名論點生成步驟中進行生成之署名論點 Kdav 用以執行資料之署名處理的步驟。

6.2. 如申請專利範圍第 5.8 項所記載之資料處理方法，其中前述論點生成步驟，

係將辨號處理對象之裝置或資料之識別資料至少一部分作為信息，並用前述主論點作為前述論點進行應用之辨號處理。

6.3. 如申請專利範圍第 6.2 項所記載之資料處理方法，其中前述辨號處理所適用 DRS 認證之辨號處理，

6.4. 一種資料處理方法，由提供存儲信息資料之存儲信息資料提供裝置，及進行存儲信息資料之利用的存儲信息資料利用裝置所構成資料處理系統中之資料處理方法，其特征在於：

前述存儲信息資料提供裝置，係根據為用以生成適用於存儲信息資料之辨號處理的存儲信息資料記述論點之記述論點生成步驟，及從提供存儲信息資料之識別子用以生成前述辨號處理對象之辨號。

本辦法規定之中國國家標準 (CNB) A4 尺寸 (210×297 毫米) - 280 -

## 六、中華專利範圍

存儲信息識別子用以生成存儲信息資料記述論點，並用以執行存儲信息資料之辨號化處理。

而前述存儲信息資料利用裝置，係根據前述記述論點生成主論點，及提供存儲信息資料之識別子的存儲信息識別子用以生成存儲信息資料記述論點，並用以執行存儲信息資料之辨號化處理。

6.5. 如申請專利範圍第 6.4 項所記載之資料處理方法，其中前述存儲信息資料提供裝置，係具有前述數不同之記述論點生成或用主論點為用以生成複數不同之存儲信息資料記述論點，並根據該複數之記述論點生成或用主論點及前述存儲信息識別子用以生成複數不同之存儲信息資料記述論點，藉由該生成之複數的記述論點用以執行辨號化處理並用以生成複數種存儲化存儲信息資料。

而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置有的複數不同之記述論點生成或用主論點至少 1 個的記述論點生成或用主論點。使用自己所有之記述論點生成或用主論點及同樣記述論點生成或用主論點由該生成之記述論點將唯化存儲化存儲信息資料進行辨號。

6.6. 一種資料處理方法，係指由複數之資料處理與複數構成資料處理系統中之資料處理方法，其特徵在於具有：

在前述複數之資料處理裝置中之一個資料處理裝置 A 中，係根據存儲信息識別子生成或用論點為用以生成適用於存儲信息資料之辨號處理的存儲信息識別子，及該資料處理

## 六、中華專利範圍

裝置 A 之辨號處理對象由該生成之存儲信息識別子將被階級化之存儲信息資料寄納於記述論點之步驟。

在不同資料處理裝置 B 中，根據前述資料處理裝置 A 及同一之前述存儲信息識別子生成或用主論點及前述資料處理裝置 A 之辨號處理對象由該生成前述存儲信息識別子及同一存儲信息識別子之記述論點生成步驟，及

在前述資料處理裝置 B 藉由之後之存儲信息識別子進行寄納於前述記述論點之存儲信息資料之辨號化的步驟。

6.7. 一種資料處理方法，由主裝置，及形成該主裝置之記述論點處理對象的副裝置所構成之資料處理系統中之資料處理方法，

前述資料處理裝置，係根據辨號論點生成用主論點為用以生成適用於主裝置及副裝置間之記述論點之記述論點，及該副裝置之識別子的副裝置識別子用以生成辨號論點，並用以生成之記述論點寄納於該副裝置內之記述論點。

而前述主裝置，係根據前述辨號論點生成用主論點，及該副裝置裝置之記述論點的副裝置識別子用以生成辨號論點並用以執行辨號處理。

6.8. 一種程式提供裝置，係用以提供電腦程式並用以執行資料辨號化、資料辨識化、資料辨發送、認證處理、署名處理至少其中之一的增強處理並將增強處理在萬能系統上執行之程式提供裝置，其特徵在於：

前述辨號程式，係含有：

將執行增強處理必要之個別論點，根據主論點為用

**六、申請專利範圍**

以生成適用於前述論據或處理之結果，及確認處理對象之某項要求之識別資料並生成之後產生步驟；及

藉由前述論據或生成步驟根據生成之後應用以執行哈密爾頓的論據或處理方法。

6.9. 一種資料處理裝置，係藉由記憶媒體或邏輯運算提供存儲信息資料之處理的資料處理裝置，其特徵在於具有：

記憶部，用以存取資料處理裝置的：

名單驗正部，用以抽出符合於存儲信息資料中之不正確機器名單，並用以執行該名單內之項目及被容納於該選記憶之前述資料處理裝置的結果處理，及

前述部，前述模擬或處理部中之核對處理結果，若合有在前述不正確機器名單中之前述資料處理裝置子進行一致的資訊時，用以中止前述存儲信息資料之再生或將該裝置的預約處理或至少其中之一的處理執行。

7.0. 如中譯專利範圍第 6.9 項所記載之資料處理裝置，其中前述各單獨註記，另具有的時將該裝置用以執行對於該存儲信息資料的總括處理。

前述總括或處理部，

係依據被合於前述存儲信息資料之不正確機器名單之核對結果有無前述不正確機器名單之變改，並藉由該驗證，僅以形成單獨使用以執行前述對處理之構成。

7.1. 如中譯專利範圍第 7.0 項所記載之資料處理裝置，其中前述資料處理裝置，係具有不正確機器名單核對

本辦法第十九條第一項圖示標準 (CNB) A4規格 (210×297毫米)

-263-

**六、申請專利範圍**

生成編碼部，

而前述號號處理部。

係對該對象之不正確機器名單模擬或生成之後的號號處理並用以生成不正確機器名單核對值，及藉由前述號號處理部用以執行適用前述不正確機器名單核對值，及藉由前述號號處理部用以執行適用前述不正確機器名單之變改之結果。

7.2. 如中譯專利範圍第 6.9 項所記載之資料處理裝置，其中前述各單獨註記，另具有總括處理部用以執行對於該存儲信息資料之總括處理，

而前述總括或處理部，係用以執行被合於前述存儲信息資料中被轉換化之後之不正確機器名單之處理，並藉由該驗證或處理之結果對於該存儲信息資料之不正確機器名單用以執行前述對處理之構成。

7.3. 如中譯專利範圍第 6.9 項所記載之資料處理裝置，其中前述各單獨註記，另具有總括處理部用以執行與形成存儲信息資料之傳遞對象或轉送部之總括裝置的相互協調或處理，

而前述名單驗正部，

係用由前述名單驗正部根據與被執行前述記憶裝置之核對並成立認證後作為條件，而以後被合於前述存儲信息資料中不正確機器名單與被容納於前述記憶裝置之前述資料處理裝置識別子用以執行前述對處理之構成。

本辦法第十九條第一項圖示標準 (CNB) A4規格 (210×297毫米)

-264-

**六、申請專利範圍**

7.4. 一種資料處理方法，係藉由記憶媒體或邏輯運算進行並提供存儲信息資料之處理的資料處理方法，其特徵俱有：

用以抽出被合於存儲信息資料中不正確機器名單之名單抽出步驟；

藉由前述名單抽出步驟被合於前述抽出之後之名單的項目，及發尋尋於資料處理裝置內之記憶庫後的細緻資料處理資訊識別子用以執行核對處理之核對處理方法；及

前述核對處理步驟中之核對處理結果，在前述不正確機器名單中合有與前述資訊識別處理資訊子一致的資訊時，用以中止前述存儲信息資料之再生或對記錄裝置之容納為僅至其中之一的處理執行的步驟。

7.5. 如中譯專利範圍第 7.4 項所記載之資料處理方法，其中前述資料處理方法，係憑用，

而根據被合於前述存儲信息資料中不正確機器名單之核對應用以驗證有無前述不正確機器名單之變改的驗證步驟，

而藉核對處理步驟，

係藉由前述驗證步驟，僅當行到完成單獨改時進行執行，

7.6. 如中譯專利範圍第 7.5 項所記載之資料處理方法，其中前述驗證步驟，

係合對該對象之不正確機器名單模擬資料用以執行應用不正確機器名單核對值生成之後的號號處理並用以

本辦法第十九條第一項圖示標準 (CNB) A4規格 (210×297毫米)

-265-

**六、申請專利範圍**

生成不正確機器名單核對值的步驟，及

用以執行生成之後之不正確機器名單核對值，及藉合於前述存儲信息資料中不正確機器名單核對值的核對並用以驗證有無前述不正確機器名單之變改的步驟。

7.7. 如中譯專利範圍第 7.4 項所記載之資料處理方法，其中前述資料處理方法，係憑用，

而用以執行前述存儲信息資料中被轉換化之後之不正確機器名單的詳細處理之核對步驟，

而前述核對處理步驟，

係做為前述存儲信息資料之結果對於被取得之不正確機器名單用以執行前述核對處理者。

7.8. 如中譯專利範圍第 7.4 項所記載之資料處理方法，其中前述資料處理方法，係憑用，

而合併存儲信息資料之傳遞對象或轉送部與記錄裝置相互通訊處理步驟，

而前述核對處理步驟，係藉由前述核對並成立認證後做為條件用以執行前述核對處理者。

7.9. 一種存儲信息資料生成方法，藉由記憶媒體或邏輯運算對被合於記錄再生器進行並提供存儲信息資料之存儲信息資料生成方法，其特徵俱有：

做為存儲信息資料之無耗資訊形成並提供存儲信息資料之用以納為構成資料之不正確機器名單並為存儲信息資料，

本辦法第十九條第一項圖示標準 (CNB) A4規格 (210×297毫米)

-266-

## 六、申請專利範圍

8.0. 如申請專利範圍第 7 項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，選至，  
作為存儲信息資料之總管資訊，用以容納前述不正確  
機械名稱之寫成後機械名稱對稱者。

8.1. 如申請專利範圍第 9 項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，選至，  
將前述不正確機械名稱進行縮短化並用以容納於存儲  
信息資料之來源資訊中者。

8.2. 一種程式，提供媒體，用以提供電腦程式或由記憶媒體或透過媒體存儲提供存儲信息資料之處理在電腦系統上執行的程序提供媒體，其特徵在於：前述電腦程式，  
係具有：

用以抽出各於存儲信息資料中不正確機械名稱之名  
單抽出子程：

藉由前述名單抽出子程對於抽出之名單的項目，  
及被選擇於資料處理區塊內之紀錄然後前述資料處理裝  
置選取子用以執行核對過程之核對處理步驟；及

前述核對過程步驟中之核對過程時，在前述不正確  
機械名稱中各有與前述資料或經識別子進行一對的資訊時，  
而以中止前述存儲信息資料之再生到記錄機械名稱的  
過程至少其中之一之過程為止步驟。

8.3. 一種資料處理裝置，藉由記憶媒體或透過媒體  
進行被提供存儲信息資料之機械的資料處理裝置，其特徵  
在於其構具有：

參照各式光碟機內部結構圖(CNS) A4規格(210x297公釐) - 287 -

## 六、申請專利範圍

號號或單部，對前述存儲信息資料實行用以執行縮短處理

控制部，對前述單部處理部用以執行控制：

系統共同體，被使用於前述單部處理部中之縮短處理  
並共同於夠用該存儲信息資料之其他的資料處理與製  
造；及

裝置固有識別子至少其中之一，為了用以生成被使用  
於前述單部處理部中之縮短處理的資料處理裝置固有之裝  
置固有識別子或該裝置固有識別子：

前述單部處理部。

僅根據前述單部處理部之利用縮短兩種子系統共同  
縮短，或前述裝置固有識別子其中之一適用於前述存儲信  
息資料並用以執行該過程。

8.4. 如申請專利範圍第 8.3 項所記載之資料處理裝  
置，其中前述資料處理裝置，

係其構具有與前述於前述資料處理裝置固有之縮短其中  
之一適用於前述存儲信息資料並用以執行該過程。

8.5. 前述專利範圍第 8.3 項所記載之資料處理裝  
置，其中前述資料處理裝置，派送部，

具有記錄機械用以記錄存儲信息資料，

而前述派送部處理部。

僅將前述存儲信息資料僅放在自己之資料處理裝置並  
附有使用之利用限制時，對前述存儲信息資料使用前述裝

置參照各式光碟機內部結構圖(CNS) A4規格(210x297公釐) - 288 -

## 六、申請專利範圍

僅具有縮短用以執行縮短處理並用以生成容納資料到前述  
點記號之。

並將前述存儲信息資料將放於自己之資料處理裝置以外  
之裝置也可做為使用時，對前述存儲信息資料使用前述系  
統共同體後而用以執行該過程並用以生成容納資料到前述  
點記號裝置之構成。

8.6. 如申請專利範圍第 8.3 項所記載之資料處理裝  
置，其中前述資料處理裝置，

係具有資料處理裝置固有之譽名鑑點 Kdev，及在複數  
之資料處理裝置共同之系統譽名鑑點 Keys，

而前述點記號或複點。

將前述存儲信息資料僅放在自己之資料處理裝置用  
有使用之利用限制時並容納於前述記錄裝置時，對前述存  
儲信息資料適用前述點記號固有之譽名鑑點 Kdev 與由點號機  
用以生成點記號固有相對值。

並將前述存儲信息資料放在自己之資料處理裝置以外  
的裝置也能夠可使用並容納於前述記錄裝置時，對前述存  
儲信息資料適用前述點記號固有之譽名鑑點 Keys 後藉由點號機  
用以生成相對值。

而前述點記號。

係前述單部處理部之生成後的前述裝置固有核對值  
或前述總處理部對稱之中之一與前述存儲信息資料一起容納於  
前述記錄裝置用以執行控制。

8.7. 如申請專利範圍第 8.3 項所記載之資料處理裝

## 六、申請專利範圍

置，其中前述資料處理裝置，

係具有資料處理裝置固有之譽名鑑點 Kdev，及在複數  
之資料處理裝置共同之系統譽名鑑點 Keys，

而前述點記號或複點。

僅係在自己之資料處理裝置用以再生被附有使用之  
利用限制的存儲信息資料時，對前述存儲信息資料適用前述  
裝置固有之譽名鑑點 Kdev 後藉由點號機用以生成點記號  
或核對值，並用以執行該生成法之供應固有核對值的核  
對處理。

而放在此處的資料處理裝置之外的裝置也做為可使  
用而以再生被附有利用限制之存儲信息資料時，對前述存  
儲信息資料適用前述系統譽名鑑點 Keys 後藉由點號機用  
以生成點記號或核對值，並用以執行該生成之後的點核對值的核  
對處理。

而前述點記號。

係前述裝置固有核對值之核對成立後的，或僅使前述  
總處理部對稱之成立點將以存儲信息資料之單獨處理部  
使處理並用以再生可再生存儲資料之構成。

8.8. 如申請專利範圍第 8.3 項所記載之資料處理裝  
置，其中前述資料處理裝置，

係具有記錄資料處理裝置固有之譽名鑑點 MKdev，  
及資料處理裝置固有之譽名鑑點 MKsys，

而前述點記號。

僅根據前述資料處理裝置固有之譽名鑑點 MKsys 及

參照各式光碟機內部結構圖(CNS) A4規格(210x297公釐) - 289 -

**六、申請專利範圍**

向該資料處理系統提出名稱號 Kdev，而由該數處理做為資料處理裝置固有號碼以用以生成其名稱號 Kdev。

9.3. 如中請專利範圍第 8.5 項所記載之資料處理裝置，其中前述裝置固有名稱號 Kdev。

係對前述資料處理裝置而將別子 IDdev 用於前述資料處理裝置固有名稱號 Kdev 之後再由 D E S 程號處理用以生成前述各名稱號之構成。

9.4. 如中請專利範圍第 8.3 項所記載之資料處理裝置，其中前述裝置固有名稱號。

係對前述存儲信息資料所以執行前述號碼並用以生成中間號碼，在該中間號碼於前述資訊資料處理裝置固有名稱號系統就有論點後用以執行暗號處理。

9.5. 如中請專利範圍第 9.0 項所記載之資料處理裝置，其中前述暗號處理。

係將前述存儲信息資料分割成複數部分後之部分資料對合 1 以上之部分資料集合藉由前述處理用以生成部分核對值。

百合生成之後之部分核對值對前述部分核對值集合資料並非由暗號處理用以生成中間號對值之構成。

9.6. 一種資料處理方法，藉由記錄媒體或訊訊媒體進行傳送存儲信息資料之處理的資料處理方法，其特徵在於：

根據前述存儲信息資料之利用規律，  
用以選擇利用前述存儲信息資料之後於其他資料處理

本說明文適用中國國家標準 ( CNS ) A4 規格 ( 319×210 毫米 ) - 291 -

**六、申請專利範圍**

用以生成裝置固有號對值。

將前述存儲信息資料放在自己之資料處理裝置以外的裝置固有名稱號可用於存放於前述記錄裝置時，對前述存儲信息資料用於前述系統名稱號 Keys 後藉由暗號處理用以生成號碼對值。

並將前述生成之後之號碼對值或前述號碼對值之一與前述存儲信息資料一起寄於前述記錄裝置。

9.6. 如中請專利範圍第 9.2 項所記載之資料處理方法，係前述資料處理方法中之存儲信息資料的再生處理中。

僅放在自己之資料處理裝置用以再生後使用之利用限制後的存儲信息資料時，對前述存儲信息資料用於前述裝置固有名稱號 Kdev 後藉由暗號處理用以生成號碼對值，並用以執行該生成之後之號碼對值的核對值的處理。

而放在自己之資料處理裝置以外之裝置被視為可使用附用限制後用以再生存儲信息資料時，對前述存儲信息資料用於前述系統名稱號 Keys 後藉由暗號處理用以生成號碼對值，並用以執行該生成之後之號碼對值的處理。

成立前述裝置固有名稱號之後，或僅成立前述號碼對值之候對後用以執行存儲信息資料之再生。

9.7. 如中請專利範圍第 9.2 項所記載之資料處理方

本說明文適用中國國家標準 ( CNS ) A4 規格 ( 319×210 毫米 ) - 292 -

**六、申請專利範圍**

依據前述資料處理系統提出名稱號，或，資料處理裝置固有名稱固有號碼其中之一的號碼或號碼。

前述原固有名稱號處理號碼用於前述存儲信息資料用以執行暗號處理。

9.3. 如中請專利範圍第 9.2 項所記載之資料處理方法，其中前述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中。

將前述存儲信息資料放於自己之資料處理裝置並限制，對前述存儲信息資料使用前述資料處理裝置用以執行暗號處理並用以生成存儲信息資料的前述記錄裝置。

而前述存儲信息資料也放在自己之資料處理裝置以外之裝置並可被用於，對前述存儲信息資料使用前述資料處理裝置並用以執行暗號處理並用以生成存儲信息資料的前述記錄裝置。

9.4. 如中請專利範圍第 9.2 項所記載之資料處理方法，對前述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中。

將前述存儲信息資料僅放在自己之資料處理裝置附有使用之利用限制並寄於前述記錄裝置時，對前述存儲信息資料用於前述裝置固有名稱號 Kdev 後藉由暗號處理

本說明文適用中國國家標準 ( CNS ) A4 規格 ( 319×210 毫米 ) - 293 -

**六、申請專利範圍**

指，合併前述資料處理裝置固有名稱號用主線號 MKdev 及資料處理裝置固有名稱號子 IDdev 相由暗號處理做為資料處理裝置固有名稱號 Kdev 之步驟。

9.5. 和中請專利範圍第 9.7 項所記載之資料處理方法，其中前述裝置固有名稱號 Kdev 生成步驟。

係對前述資料處理裝置固有名稱號子 IDdev 用於前述資料處理裝置固有名稱號用主線號 MKdev 後藉由 D E S 程號處理用以生成前述裝置固有名稱號 Kdev 之步驟。

9.6. 如中請專利範圍第 9.2 項所記載之資料處理方法，其中前述資料處理方法，係前述。

對前述存儲信息資料分割成複數部分後之部分資料對合 1 以上部分資料集合藉由暗號處理用以生成部分核對值。

並對前述生成之後之部分核對值的部分核對值集合資料藉由暗號處理用以生成中間號對值。

1.0.1. 一種程式提供錄帶，提供兩種程式由記憶體或訊訊媒體進行被提供存儲信息資料之處理將資料處理在電腦系統上執行之程式提供錄帶，其特徵在於：

並對前述存儲信息資料分割成複數部分後之部分核對值的部分核對值集合資料藉由暗號處理用以生成中間號對值。

成立前述裝置固有名稱號之後，或僅成立前述號碼對值之候對後用以執行存儲信息資料之再生。

9.7. 如中請專利範圍第 9.2 項所記載之資料處理方

本說明文適用中國國家標準 ( CNS ) A4 規格 ( 319×210 毫米 ) - 294 -

## 六、中請專利範圍

前述電腦程式。

係根據前述存儲信息資料之利用態樣。

用以選擇並列存儲信息資料共同於其他資料處理裝置之時將處理所用系統共同操作，或，資料處理與儲存有之變更因有備此其中之一的確號或證據之步驟。

將選擇之後之確號或證據適用於前述存儲信息資料用以執行該項處理之步驟。

102. 一種資料處理裝置，藉由記錄媒體或通訊媒體進行傳遞存儲信息資料之技術的資料處理裝置，其特點在於其具有：

储存處理部，對前述存儲信息資料用以執行增號處理；及

增號部，對前述存儲處理部用以執行性別。

前述增號處理部。

係在會於資料統計對象之存儲信息資料單位用以生成存儲信息對值，藉由用以執行生成後之存儲信息統計對象之對應，用以執行前述資料中之存儲信息區段資料的正當性驗證處理之構成。

103. 如中請專利範圍第102項所記載之資料處理裝置，其中前述資料處理裝置，係具有存儲信息對值生成編址。

前述增號處理部。

係依據驗證對象之存儲信息區段資料用以生成存儲信息中間值，並對前述存儲信息中間值適用前述存儲信息對值。

A5版式適用中國國家標準 (CN) A4紙 (210x297mm)

## 六、中請專利範圍

號生成編址後用以執行增號處理並用以生成存儲信息對值之構成。

104. 如中請專利範圍第103項所記載之資料處理裝置，其中前述增號處理部，藉由存儲信息區段資料之確號處理將被取錄詳文全體以預定組元單位進行預定之演算處理並用以生成存儲信息中間值。

使驗證對象之存儲信息區段資料未被縮小化時，將存儲信息區段資料全體以預定組元單位進行預定之演算處理用以生成存儲信息中間值之構成。

105. 如中請專利範圍第104項所記載之資料處理裝置，其中前述增號處理部中之前述中規則對值的生成處理進行適用前述第104項所記載之演算處理並用以生成存儲信息中間值之構成。

106. 如中請專利範圍第104項所記載之資料處理裝置，其中前述增號處理部，

係藉由C B C模式具有增號處理之構成。

並使驗證對象之存儲信息區段資料將被縮小化時適用於存儲信息中間值生後處理之前述增號處理，藉由C B C模式之譯碼過程。

107. 如中請專利範圍第108項所記載之資料處理裝置，其中前述增號處理部具有C B C模式的增號處理構成，並稱存儲在形成處理對象之信息列的一部分。

A5版式適用中國國家標準 (CN) A4紙 (210x297mm)

## 六、中請專利範圍

前述選用複數共同檢驗對值之構成。

108. 如中請專利範圍第102項所記載之資料處理裝置，其中前述增號處理之構成。

係在存儲信息區段資料含有複數之零件，並非係於資訊儲存器資料一部分之零件有驗證對值時，根據驗證對象零件用以生成存儲信息對值，並藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之存儲信息對值與資料單位的正當性驗證處理之構成。

109. 如中請專利範圍第108項所記載之資料處理裝置，其中前述增號處理。

係在前述存儲信息區段資料含有複數之零件，使驗證對象之要驗證零件有1至1時。

使前述要驗證零件被驗證時，藉由要驗證零件之譯碼過程並取錄詳文全體以預定組元單位在進行將危險和後之值，適用存儲信息對值生成並後用以執行增號處理並用以生成存儲信息對值。

並前述要驗證零件未被縮小化時，將該要驗證零件全體以預定組元單位將危險和後之值，適用前述存儲信息對值生成並後用以執行增號處理並用以生成存儲信息對值之構成。

110. 如中請專利範圍第108項所記載之資料處理裝置，其中前述增號處理。

係在前述存儲信息區段資料含有複數之零件，使驗證對象之要驗證零件有複數時。

A5版式適用中國國家標準 (CN) A4紙 (210x297mm)

## 六、中請專利範圍

在各零件適用各存儲信息對值生成並用以執行增號處理對象之零件之譯碼資料，進而適用前述存儲信息核對值後用以執行增號處理將被取得結果作為存儲信息對值之構成。

111. 如中請專利範圍第102項所記載之資料處理裝置，其中前述存儲信息處理裝置，係述即：

具有記憶装置在前述增號處理部中用以容納存儲信息資料可供執行正確性驗證後之存儲信息區段資料。

112. 如中請專利範圍第111項所記載之資料處理裝置，在前述增號處理部中之存儲信息對值的核對處理中，在未成立核對後之情形中，

前述控制部，係具有用以中止並刪除此記錄裝置之構成。

113. 如中請專利範圍第102項所記載之資料處理裝置，其中前述增號處理部用以再生被執行正確性驗證後之資料。

114. 如中請專利範圍第113項所記載之資料處理裝置，其中前述存儲信息處理裝置，

係在前述增號處理部中之存儲信息對值的核對處理中，在未成立核對後之情形中，

前述控制部，其構成具有在前述再生處理部用以中止再生處理者。

115. 一種資料處理方法，藉由記錄媒體或通訊媒

A5版式適用中國國家標準 (CN) A4紙 (210x297mm)

## 六、申請專利範圍

關進行發被提供存儲信息資料之處理的資料處理方法。

係在於資料驗證對象之存儲信息區段資料單位用以生成存儲信息核對值，藉由用以執行生成後之存儲信息核對值之依賴對處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗證步驟。

1 1 6 . 如申請專利範圍第 1 1 5 項所記載之資料處理方法，其中前述資料處理步驟，

係根據驗證對象之存儲信息區段資料用以生成存儲信息中問題。

並對生成後之存儲信息中問題用存儲信息核對值後用以執行確認或識別並用以生成存儲信息核對值。

1 1 7 . 如申請專利範圍第 1 1 5 項所記載之資料處理方法，其中前述資料處理步驟，

係依據對象之存儲信息區段資料基準號化時，藉由該存儲信息區段資料之譯碼處理並藉由譯碼全文體以預定祖先單位進行預定之演算處理並用以生成存儲信息中異質。

並使驗證對象之存儲信息區段資料被縮小化時，將存儲信息區段資料全體以預定祖先單位進行預定之演算處理並用以生成存儲信息中異質。

1 1 8 . 如申請專利範圍第 1 1 7 項所記載之資料處理方法，其中前述資料處理步驟，

在前述中間核對值的生成過程中進行適用前述預定之演算處理係係他之性態和次序。

本件各式送達中國國家知識產權局 (CNIPA) A4紙張 (210×297公釐) -209-

## 六、申請專利範圍

號處理並用以生成存儲信息核對值。

前述驗證對象件之差異物化時，將該對象件全體以預定祖先單位進行預定並後之值，藉由用以生成存儲信息核對值並生成點化並用以執行單號處理並用以生成存儲信息核對值。

1 2 3 . 如申請專利範圍第 1 2 1 項所記載之資料處理方法，其中前述資料處理方法中，

在前述存儲信息區段資料被含有複數之零件，使驗證對象之存儲信息區段資料再被複數之零件，

在各零件適用存儲信息核對值生成點化用以執行單號處理並取後之零件被預定之運算資料，並而用以生成存儲信息核對值並生成點化後用以執行單號處理並取得點化為存儲信息核對值。

1 2 4 . 如申請專利範圍第 1 1 5 項所記載之資料處理方法，其中前述資料處理方法，係述面。

合基執行正當性驗證後之存儲信息區段資料合用以容納存儲信息資料的步驟。

1 2 5 . 如申請專利範圍第 1 2 4 項所記載之資料處理方法，其中前述資料處理方法，係述面。

在存儲信息核對值之抵消處理中，在未成立核對後之情形。

前述抵消部，係用以中止客倉處理到前述記錄裝置。

1 2 6 . 如申請專利範圍第 1 1 5 項所記載之資料處理方法，其中前述資料處理方法，係述面。

本件各式送達中國國家知識產權局 (CNIPA) A4紙張 (210×297公釐) -301-

## 六、申請專利範圍

1 1 9 . 如申請專利範圍第 1 1 7 項所記載之資料處理方法，其中前述存儲信息中問題之生成過程中，

使驗證對象之存儲信息區段資料被縮小化並用於存儲信息中問題生成處理之前述譯碼處理，係由 C B C 模式之譯碼處理。

1 2 0 . 如申請專利範圍第 1 1 9 項所記載之資料處理方法，其中前述由前述 C B C 模式之譯碼處理構成，係僅在形成處理對象之信息列的一部分運用複數次共同論點並以此為處理。

1 2 1 . 如申請專利範圍第 1 1 5 項所記載之資料處理方法，其中前述資料處理方法中，

在存儲信息區段資料含有複數之零件，並使該合於該存儲信息區段資料之一部分之零件有據對象時，根據驗證對象使用用以生成存儲信息核對值。

並藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之存儲信息區段資料單位的正當性驗證處理。

1 2 2 . 如申請專利範圍第 1 2 1 項所記載之資料處理方法，其中前述資料處理方法中，

在前述存儲信息區段資料被含有複數之零件，使驗證對象之要驗證零件有 1 個時，

後第步要驗證零件被縮小化時，藉由要驗證零件之譯碼處理並取得譯碼全文體以預定祖先單位在進行該步運算和後之步，通過存儲信息核對值生成點化後用以執行該步。

本件各式送達中國國家知識產權局 (CNIPA) A4紙張 (210×297公釐) -300-

## 六、申請專利範圍

合用以再生被執行正當性驗證後之資料用以執行再生處理之步驟。

1 2 7 . 如申請專利範圍第 1 2 6 項所記載之資料處理方法，其中前述資料處理方法，

係在存儲信息核對值之核對過程中，在未成立核對後之情形中，用以中止客倉處理。

1 2 8 . 一種存儲信息資料驗證方法，為了存儲信息資料驗證處理之存儲信息資料驗證方法，其特徵為：

在該合於資料驗證對象之存儲信息區段資料單位以生成存儲信息核對值，並而生成後之存儲信息核對值合被認對象存儲信息區段資料賦予存儲信息資料。

1 2 9 . 如申請專利範圍第 1 2 8 項所記載之存儲信息資料驗證方法，其中前述存儲信息核對值，係指驗證對象之存儲信息區段資料用以生成存儲信息中某個對該存儲信息核對值生成點化。

1 3 0 . 如申請專利範圍第 1 2 8 項所記載之存儲信息資料驗證方法，其中前述存儲信息核對值，係指驗證對象之存儲信息區段資料用以生成存儲信息中某個對該存儲信息核對值生成點化後用以執行單號處理並生成之值。

1 3 1 . 如申請專利範圍第 1 2 6 項所記載之存儲信息資料驗證方法，其中前述存儲信息核對值，係指驗證對象之存儲信息區段資料用以執行單號處理並生成之值。

本件各式送達中國國家知識產權局 (CNIPA) A4紙張 (210×297公釐) -302-





## 六、中情專利範圍

取出用以執行譯碼處理並由生成譯碼資料 Kcon。

而對該生成後之譯碼資料 Kcon 通常用不同類號譯匙 Kstr 產生由以執行類號處理，及根據類號譯匙 Kstr 用以生成被暗號處理過後之輸出號譯匙資料 Ktr [ Kcon ]。

而前述生成後之母譯匙資料 Ktr [ Kcon ] 寄納到前述存儲器資訊資料之集管部，並與前述該點之存儲信息區段一起寄納於前述記錄步驟。

151. 一種資料處理方法，具有使至少一部分之密語始祖暗化後之複數的存儲信息區段，及用以寄納有關於存儲信息區段之資訊的集管部對存儲信息資料之記錄並應用以執行存儲處理的資料處理方法。

係將前述記錄號譯匙據以使據於形成資訊寄納到之存儲信息資料之存儲信息區段，藉由暗號譯匙 Kble 被暗化後之存儲信息，及根據暗號譯匙 Kdis 由被暗化後之暗號譯匙資料 Kdis [ Kble ] 並構成。其特徵在於：

前述前述記錄號譯匙資料 Kdis [ Kble ] 由前述集管部進行取出，用以執行該暗號譯匙 Kble 處理並用以生成譯碼資料 Kble。

而對該生成後之譯碼資料 Kble 通常用不同類號譯匙 Kstr 由用以執行類號處理，及根據類號譯匙 Kstr 用以生成被暗號處理過後之輸出號譯匙 Ktr [ Kble ]。

而前述生成後之輸出號譯匙資料 Ktr [ Kble ] 寄納到前述存儲信息區段，並與複數之存儲信息區段一起寄納於前述記錄步驟。

本說明文是適用中國國家標準 ( CNS ) A4規格 ( 210×297公釐 )

-311-

## 六、中情專利範圍

而使用被合於被記錄後之存儲信息資料的伸長處理程式用以執行統合於該存儲信息資料之壓縮存儲信息的伸長處理，。

154. 如中情專利範圍第 153 項所記載之資料處理步驟，其中資料處理裝置，係進而具有：

資料記憶部，藉由前述存儲信息資料分析部用以寄納被抽出後之壓縮存儲信息；及

程式記憶部，藉由前述存儲信息資料解密部用以寄納被抽出後之伸長處理程式；

而前述伸長處理部。

而對被記錄於前述資料記憶部後之壓縮存儲信息，適用用記憶於前述程式記憶部之後之伸長處理程式並用以執行伸長處理。

155. 如中情專利範圍第 153 項所記載之資料處理裝置，其中前述存儲信息資料分析部其構成係，

被擴合於前述存儲信息資料之集管部實質用以取得存儲信息資料之構成資訊並進行存儲信息資料之解密者。

156. 如中情專利範圍第 155 項所記載之資料處理裝置，其中在前述無存儲資訊。

而係合壓縮存儲信息之再生優先級資訊。

並在前述伸長處理部中從前存儲處理對象之壓縮存儲信息有複數時。

而前述伸長處理部，係在從所述存儲信息資料解析部根據取得後之壓縮資訊中的優先級資訊，依從該優先級

本說明文是適用中國國家標準 ( CNS ) A4規格 ( 210×297公釐 )

-313-

## 六、中情專利範圍

152. 一種程式提供媒體，用以提供複數程式具有使至少一部分之高頻存儲量化後之複數的存儲信息區段，及用以寄納有關存儲信息區段之資訊的集管部對存儲信息資料之記錄並從存儲器納資料之生成過程在電腦系統執行之程式提供演算，而前述電腦程式，

係對前述記錄媒體而形成寄納對象之存儲信息資料，將前述存儲信息區段之暗號譯匙 Kccb 由被暗化後之 Kdis 將暗號處理後之後之暗號譯匙資料 Kdis [ Kcon ] 由前述納於前述集管部後之資料被構成，其特徵在於：

將前述暗號譯匙資料 Kdis [ Kcon ] 由前述集管部進行取出用以執行譯碼處理並用以生成譯碼資料 Kcon 之步驟。

而對該生成後之譯碼資料 Kcon 通常用不同類號譯匙 Kstr 由用以執行類號處理，根據類號譯匙 Kstr 用以生成被暗號處理後之前之暗號譯匙 Ktr [ Kcon ] 之步驟。

將前述生成功能號譯匙資料 Ktr [ Kcon ] 寄納到前述存儲信息資料之集管部之步驟。

153. 一種資料處理裝置，藉由記憶裝置或透過訊號處理部以提供之存儲信息資料的再生處理之資料處理裝置，其特徵在於真：

存儲信息資料解析部，含被壓縮後之存儲信息及依據被壓縮信息之伸長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理程式之抽出來處理；及

伸長處理部，被為自前述存儲信息資料解析部之解析達

本說明文是適用中國國家標準 ( CNS ) A4規格 ( 210×297公釐 )

-312-

## 六、中情專利範圍

位用以執行順序存儲信息對象處理之情形。

157. 如中情專利範圍第 153 項所記載之資料處理裝置，其中資料處理裝置，係進而具有：

顯示裝置，用以顯示形成待存取對象之壓縮存儲信息的資訊；及

輸入裝置，由被顯示於前述顯示裝置之待存取存儲信息資料用以輸入被著錄後之再生存儲信息對象資料；

而前述存儲處理部。

係由前述裝合於壓縮存儲裝置輸入後之再生存儲信息對象資料，用以執行對應於該對象資料之壓縮存儲信息的待存取處理之構成。

158. 一種資料處理裝置，若由記憶裝置或透過訊號處理部以提供之存儲信息資料的再生處理之資料處理裝置，其特徵在於：

用以被合壓縮存儲信息，或伸長處理程式其中之一的存儲信息資料，由被合於接收存儲信息資料之集管資訊使該存儲信息資料用以判別壓縮存儲信息或伸長處理程式之構成。

後該存儲信息資料有壓縮存儲信息符，由該存儲信息資料之集管資訊，用以取得被適用於該壓縮存儲信息符之壓縮處理程式之構成，並具有：

存儲信息資料解析部，使該存儲信息資料具有伸長處理程式，由該存儲信息資料之集管資訊用以取得伸長處理程式之構成；及

本說明文是適用中國國家標準 ( CNS ) A4規格 ( 210×297公釐 )

-314-



## 六、申請專利範圍

選擇步驟，在前述存儲信息資料解析步驟中對解析後之存儲存儲信息的變換處理程式類型將可適用之仲長處理程式，當前述存儲信息資料解析步驟根據被解析後之仲長處理程式選擇加以選擇；及

仲長處理步驟，在前述選擇步驟中藉由選擇後之仲長處理程式以執行仲長處理：

1.6.9. 如申請專利範圍第1.6項所記載之資料處理方法，其中前述資料處理方法，係述而具有：

資料型態步驟，藉由前述存儲信息資料解析部用以客觀地檢出後之歷經存儲信息；及

假設選擇步驟，藉由前述存儲信息資料解析部用以客觀地檢出後之仲長處理程式；

而前述存儲信息步驟；

保在前述資料型態步驟並記憶後之歷經存儲信息，並於前述記憶步驟中適用被記憶後之仲長處理程式並用以併存處理；

1.7.0. 如申請專利範圍第1.6項所記載之資料處理方法，其中在該處異常資訊，

係保有歷經存儲信息之再生後先順位資訊，使形成仲長處理對象之歷經存儲信息有複數時，

則前述仲長處理步驟；

係於前述存儲信息資料解析步驟中根據被取得後之集管資訊中的優先順位資訊，依從優先順位進行順序執行；

本件以尺寸規格圖面積(CNS A4規格)(210×297公釐)

-319-

## 六、申請專利範圍

1.7.1. 如申請專利範圍第1.6.8項所記載之資料處理方法，其中前述資料處理方法，係述而具有：

檢索步驟用以檢索仲長處理程式，而前述檢索步驟，

係在前述存儲信息資料解析步驟中對進行解析後之歷經存儲信息類型將可適用之仲長處理程式，將可存取之程式的尋找依據為後檢索並進行檢索；

1.7.2. 如申請專利範圍第1.6.8項所記載之資料處理方法，其中前述資料處理方法，係述而具有：

檢索步驟，係將前述仲長處理對象之歷經存儲信息的資訊系統於顯示屏；及

輸入步驟，由該顯示於前述顯示裝置後之存儲信息資料用以輸入該選擇之再生存儲信息並識別資料；

而前述仲長處理步驟；

係由前述檢索入庫資訊並根據地檢出後之再生存儲信息識別資料，而以執行判斷於該選別資料之歷經存儲信息的仲長處理；

1.7.3. 一項存儲信息資料生成方法，藉由記憶體或進訊揮體進行提供之存儲信息資料的生成過程之存儲信息資料生成方法，其特徵為：

用以生成使被記憶後之各存儲信息及該歷經存儲信息之仲長處理程式組合之存儲信息資料。

1.7.4. 如申請專利範圍第1.7.3項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進

本件以尺寸規格圖面積(CNS A4規格)(210×297公釐)

-320-

## 六、申請專利範圍

而，

做為前述存儲信息資料之集管資訊用以附加前述存儲信息資料之構成資訊，

1.7.5. 如申請專利範圍第1.7.3項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

做為前述存儲信息資料之集管資訊，係用以附加前述存儲信息資料之再生後先順位資訊，

1.7.6. 一項存儲信息資料生成方法，係藉由記憶體或進訊揮體進行提供之存儲信息資料的生成過程之存儲信息資料生成方法，其特徵為：

使存儲信息資料適用以識別歷經存儲信息或仲長處理程式之存儲信息資料集組成並進行附加。

使前述存儲信息資料適用於該歷經存儲信息後將被適用於該歷經存儲信息之後之歷經處理程式僅僅係依為集管資訊並進行附加。

而前述存儲信息資料適用於該歷經存儲信息或仲長處理程式時，則將前述仲長處理程式之陳述資訊並用以生成進行附加後之存儲信息資料。

1.7.7. 如申請專利範圍第1.7.6項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

做為前述存儲信息資料之集管資訊，係用以附加前述存儲信息資料之存儲信息的再生後先順位資訊。

本件以尺寸規格圖面積(CNS A4規格)(210×297公釐)

-321-

## 六、申請專利範圍

1.7.8. 一種程式提供機體，用以供應電腦程式藉由記憶體或進訊揮體將前述存儲信息資料之再生處理在電腦系統上執行的程式提供機體，其特徵在於：製造電腦程式，係具有：

存儲信息資料解析步驟，含被記憶後之存儲信息及該歷經存儲信息之仲長處理程式用以執行前述存儲信息資料之存儲信息資料解析，並能用以執行由該存儲信息資料之歷經存儲信息，及仲長處理程式之抽出處理；及

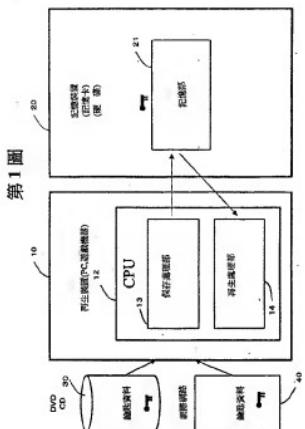
仲長處理步驟，做為前述存儲信息資料解析之剖析結果使用並於被取得後之存儲信息資料的仲長處理程式用以執行並含於該存儲信息資料之歷經存儲信息的仲長處理。

本件以尺寸規格圖面積(CNS A4規格)(210×297公釐)

-322-

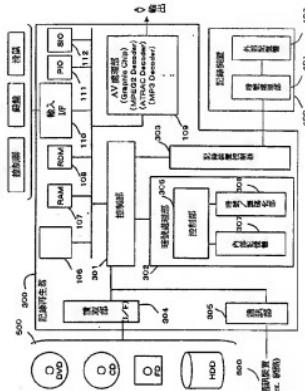
514843

739374

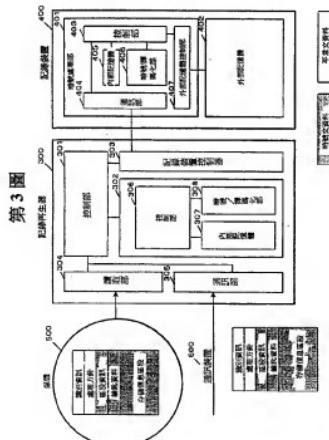


514843

第2圖

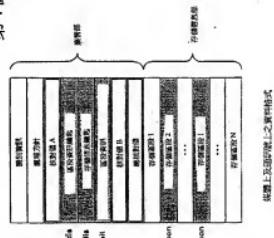


514843



514843

第4圖



半導體上元件印制佈線之接線規範

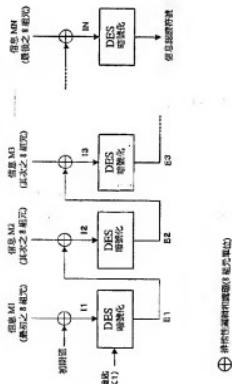
第5圖



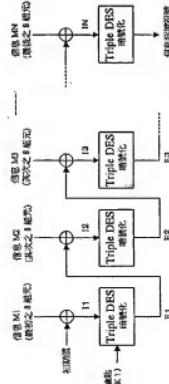
第6圖



第7圖



第8圖



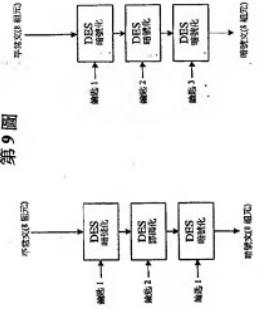
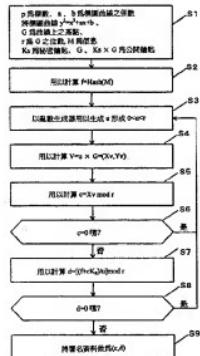
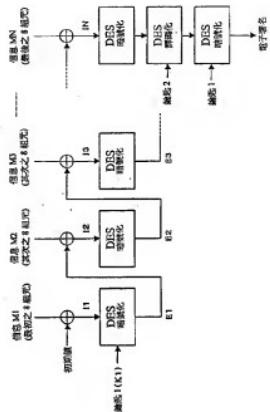


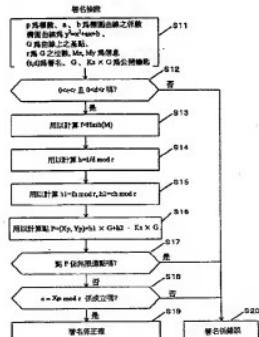
圖9第



#### 署名生成 (IEEE P1363/D3)

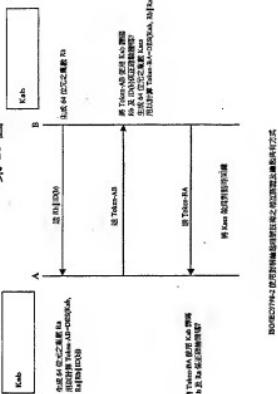


第10回

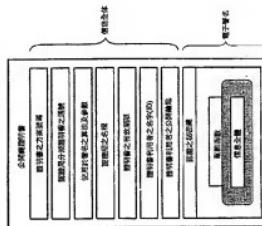


電力輸送(IEEE P1363/D3)

第 13 圖

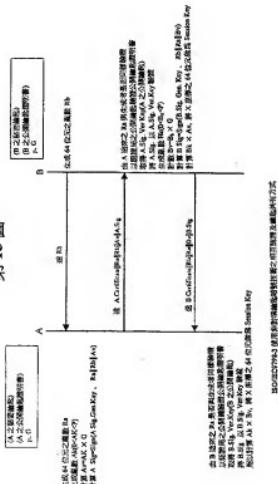


第 14 圖

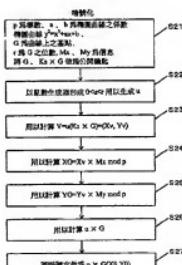


公報圖

第 15 圖



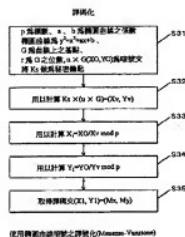
第 16 圖



此件標題並非即時之用範例(Means-Value)

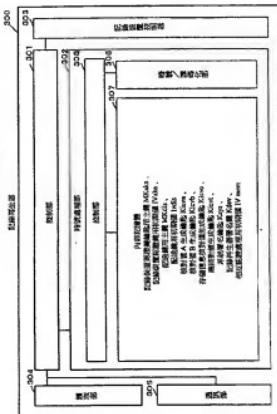
514843

第 17 圖



514843

第 18 圖



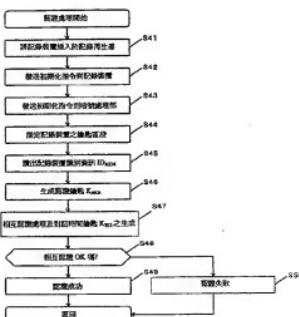
長時間計算上之資料存取

514843

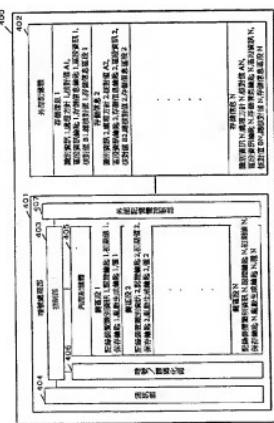
514843

514843

第 20 圖

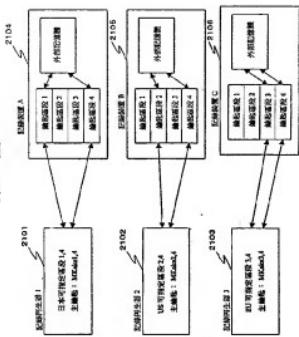


第 19 圖



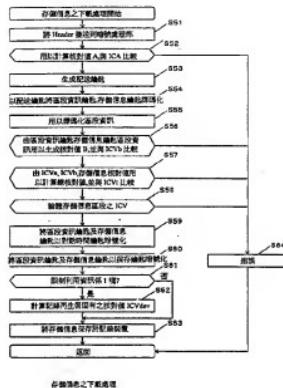
514843

第 21 圖



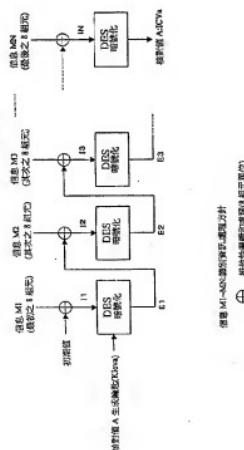
514843

第 22 圖



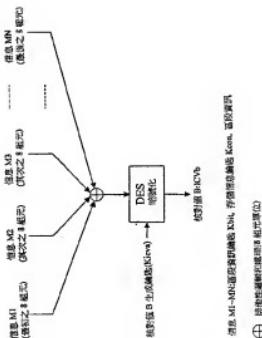
514843

第 23 圖

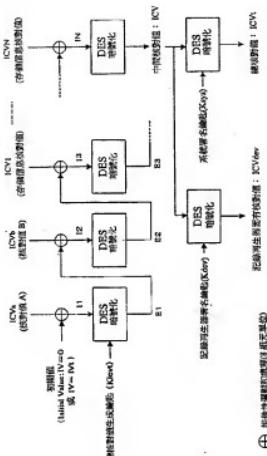


514843

第 24 圖

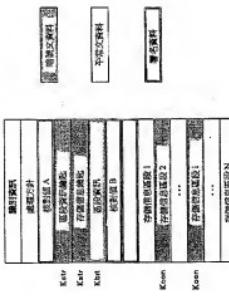


514843



514843

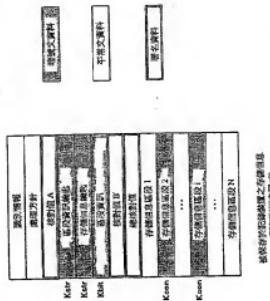
第27圖



洪武御制詩卷之十一

514843

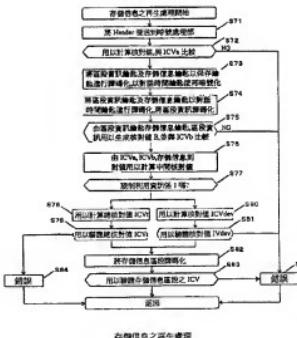
第26回



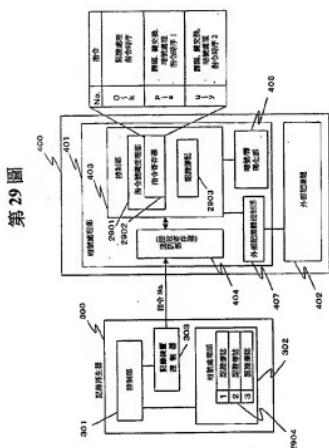
现代汉语词典(第5版)

514843

第28课

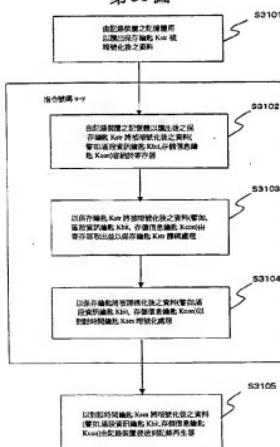


514843



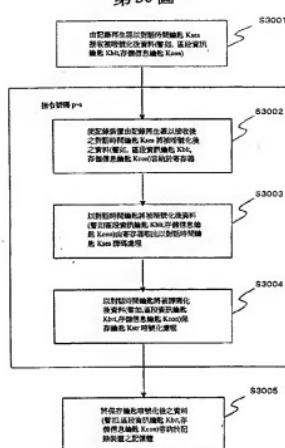
第29圖

514843



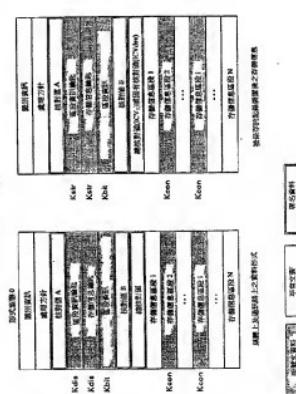
第31圖

514843



第30回

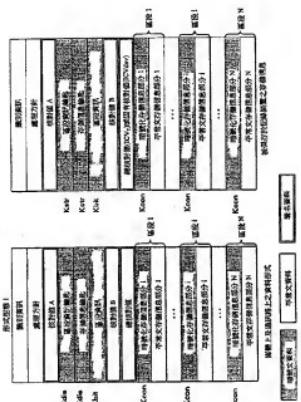
514843



第32圖

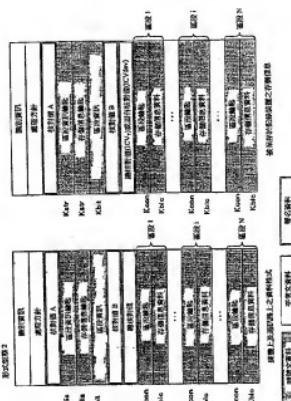
514843

第33圖



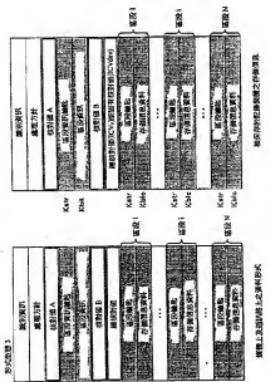
514843

第34圖



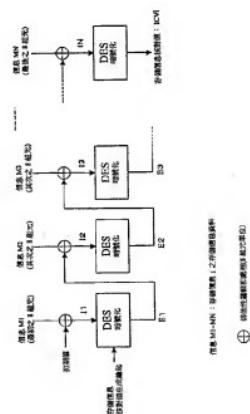
514843

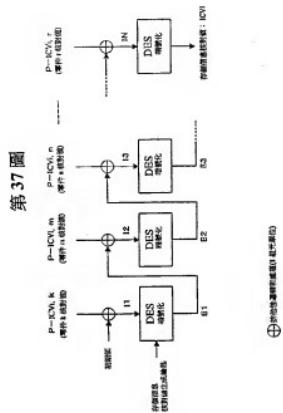
第35圖



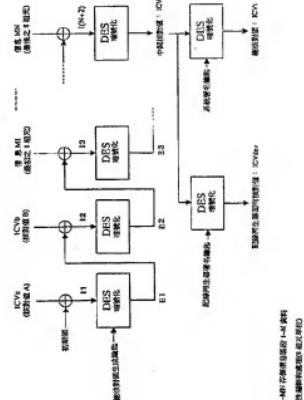
514843

第36圖



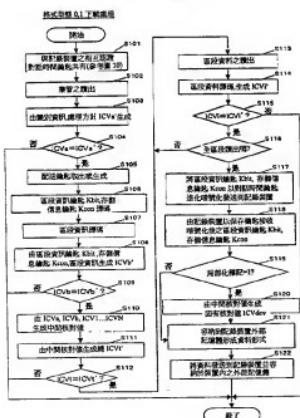


第37圖

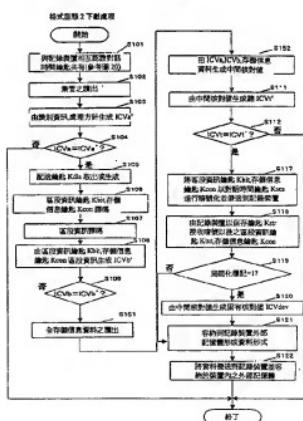


三八

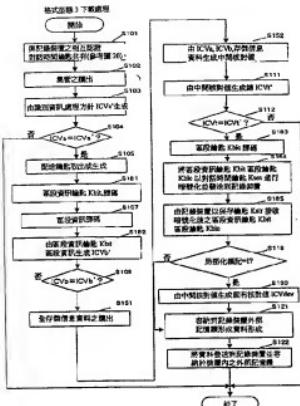
第39圖



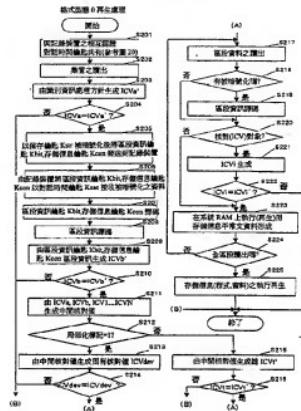
第40回



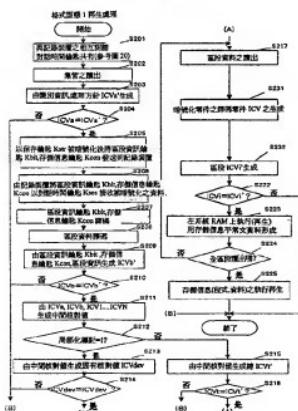
第 41 圖



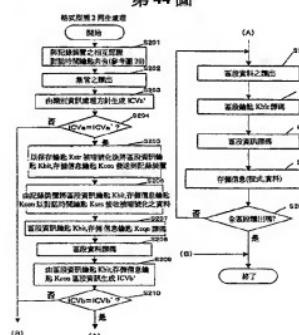
第 42 圖



第 43 圖

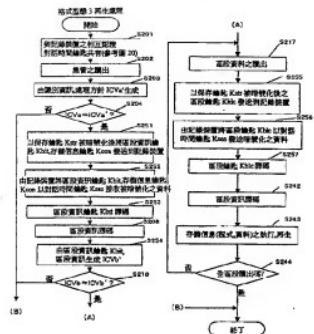


第 44 圖



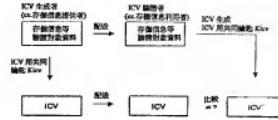
514843

第 45 圖



514843

第 46 圖

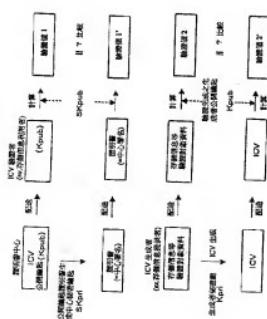


第 47 圖



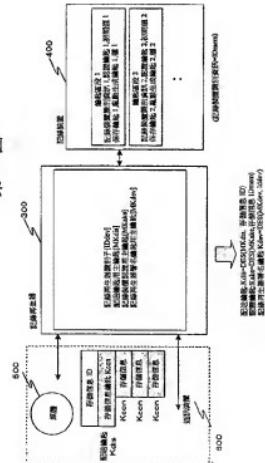
514843

第 48 圖

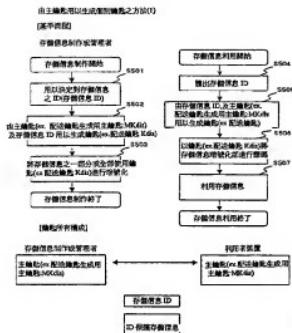


514843

第 49 圖

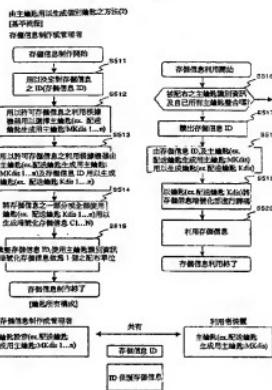


514843



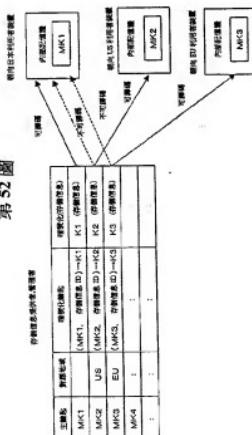
第 50 回

514843



第 51 題

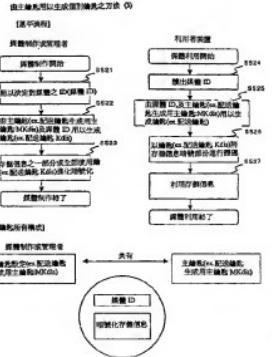
514843



第52回

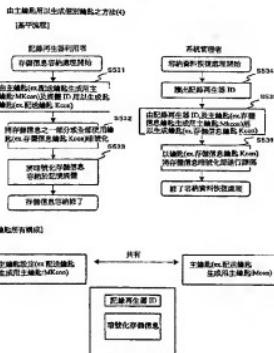
第 53 講

514843

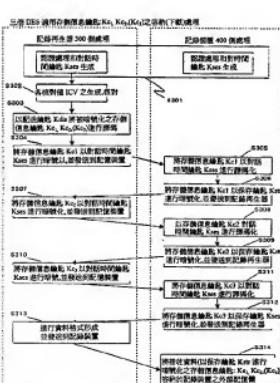


第 53 頁

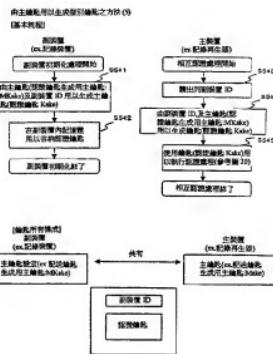
第 54 课



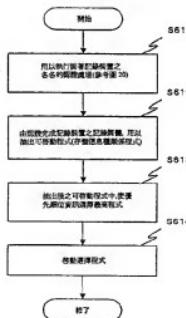
第 56 回

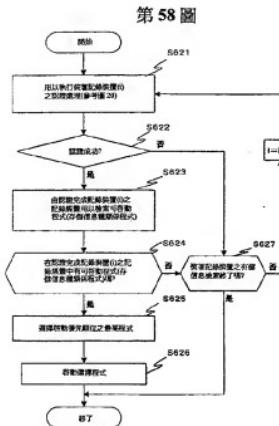


第 55 頁

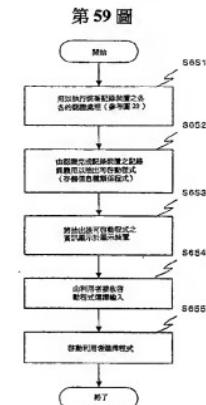


第 57 頁

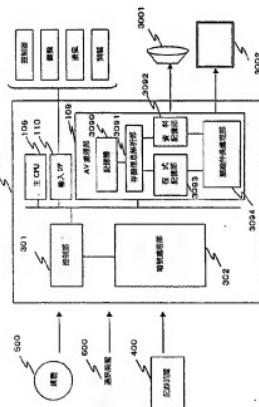




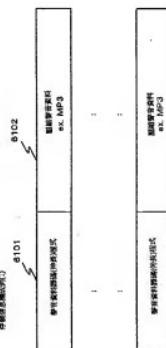
第 58 ■



第 59 題



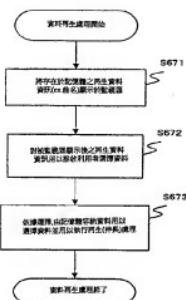
四  
60



第61回

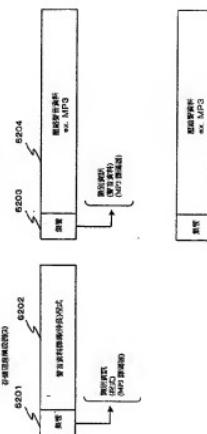
514843

第 62 圖



514843

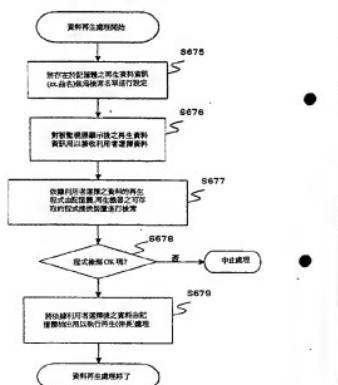
第 63 圖



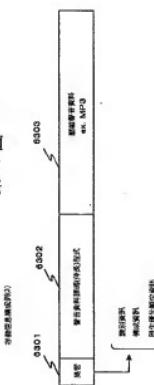
514843

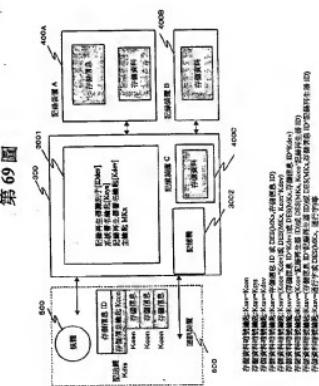
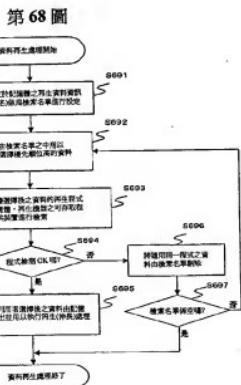
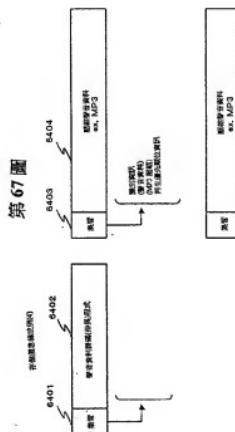
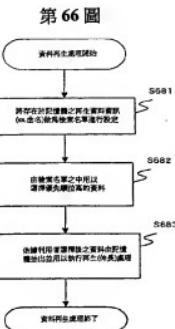
514843

第 64 圖



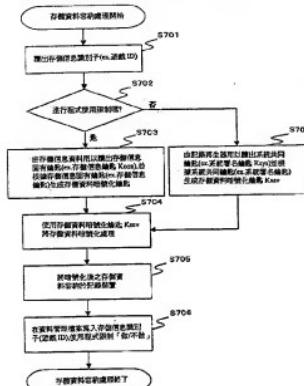
第 65 圖





第 70 圖

(2) 使用行動資料並輸出,或系統共同處理後之存儲資料的處理例

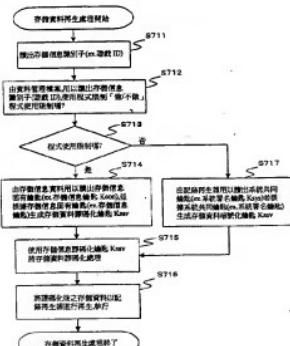


第 71 圖

存儲資料並處理		備註
步驟	說明	備註
S701	存儲資料並處理開始	..
S702	程式使用資料時？	..
S703	由於總共資料並處理時，將由系統共同處理，因此不需再進行資料整理。	..
S704	由總共資料並處理時，將由系統共同處理，因此不需再進行資料整理。	..
S705	資料整理完成。	..
S706	在資料整理後，再存入存儲資料庫。(是(S706)或不是(S706))	..
End1	存儲資料並處理終了	..

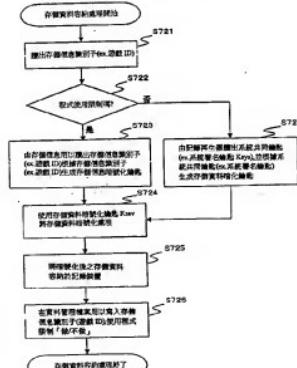
第 72 圖

(2) 使用行動資料並輸出,或系統共同處理後之存儲資料的處理例



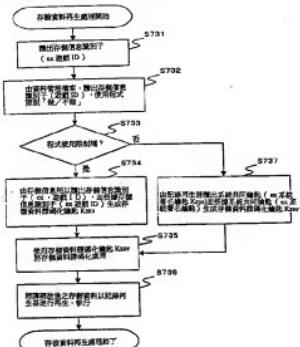
第 73 圖

(2) 使用行動資料或系統共同處理後之存儲資料的處理例



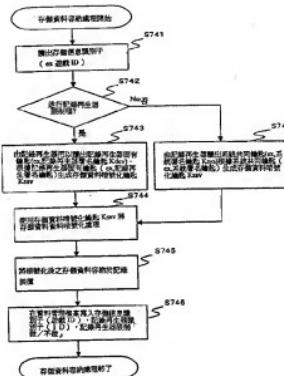
第74圖

(4) 使用存儲資料中之系統共用機制之存儲資料再生處理例



第75圖

(5) 使用記錄再生機制之存儲資料再生處理例

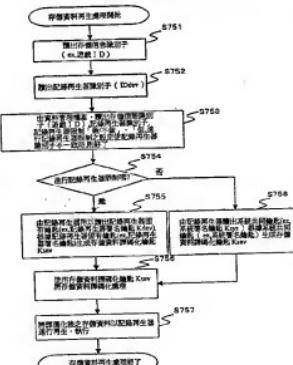


第76圖

資料庫名稱		備註		
資料庫名稱	資料庫ID	備註	備註	備註
存儲資料庫	514843...	514843...	514843...	514843...
資料庫備份	12345678...	A1C0D1E1...	12345678...	...

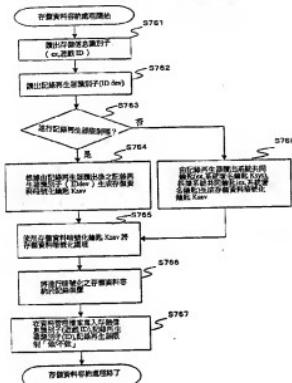
第77圖

(6) 使用記錄再生機制之存儲資料再生處理例



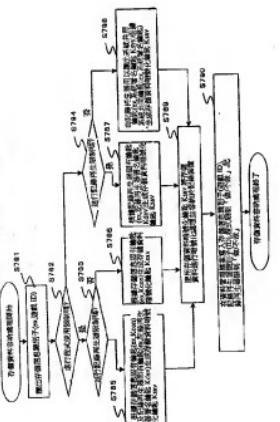
第 78 圖

(7) 使用記錄再生成陳列子。o/r 系統共同輪胎之存儲資料容納處理例



四〇八

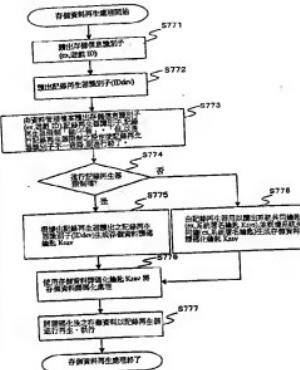
列傳第十一



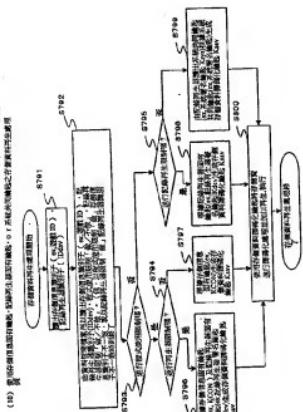
新单号		新单号	新单号	新单号
1	1	12345678...	A12345678...	新
2	2	ABCDEF12...	D898543...	新
3	3	123456789...	56531782...	不接

第 79 頁

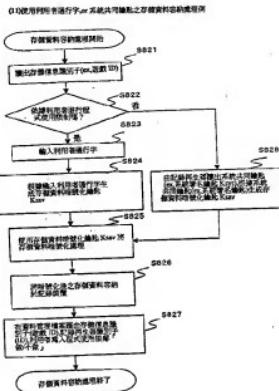
（内使用即地再生菌糲利用，系統共同  
微生物之存續及可行生産技術）



第 82 圖



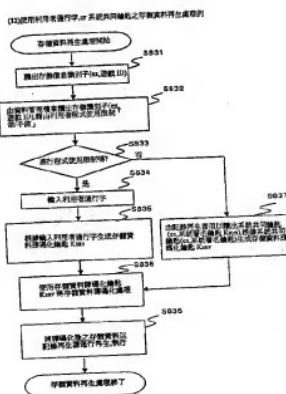
第 83 圖



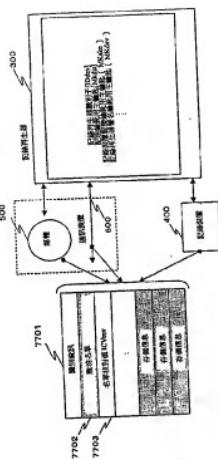
第 84 圖

序号	文件名	文件类型	文件大小
1	12345678...	报告 (Report)	7M
2	ABCDEF1...	报告 (Report)	7M
3	12345678...	报告 (Report)	7M

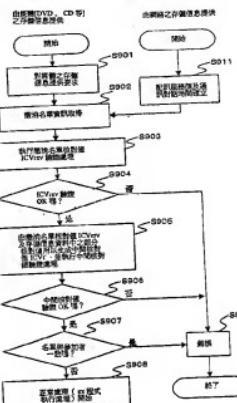
第 85 圖



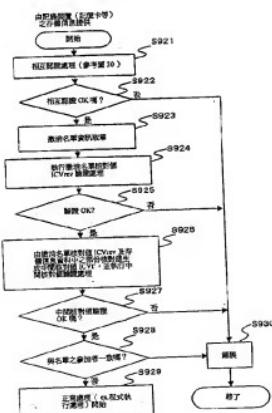
第 86 圖



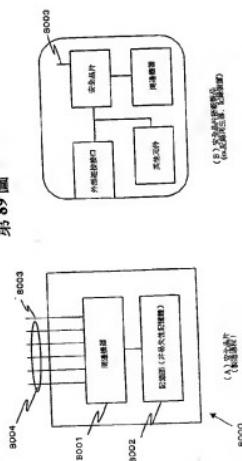
第 87 圖



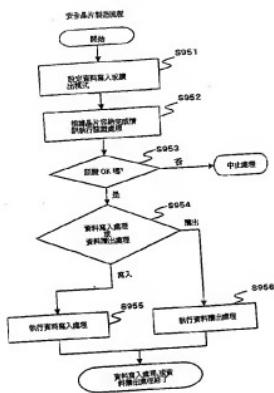
第 88 圖



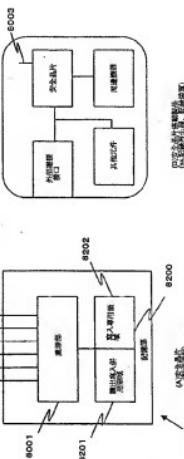
第 89 圖



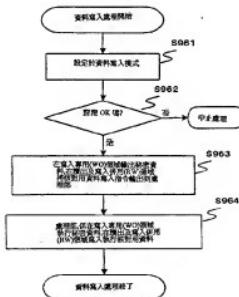
第 90 圖



第 91 圖



第 92 圖



第 93 圖

